Safe Deposit Box Insurance Coverage, LLC (SDBIC);

Incident Response Plan for Data Breaches

The Company maintains and requires its critical vendors to maintain an incident response plan designed to identify and quickly mitigate the consequence of a system breach whether through malicious or destructive spyware, malicious code or simple unauthorized access where personally identifiable customer information is compromised.

Program Coordinator

The coordinator of all IRP responses for the Company shall be Mark Mason, the COO of the Company. In the event of his unavailability, or unwillingness to act as the Program Coordinator, Gerald Pluard, CEO of the Company shall assume such responsibility.

Initial Response

Upon discovery by the Program Coordinator or receipt of notice from one of the Companies vendors that a system breach resulted in unauthorized third parties gaining access to personally identified customer information, the Program Coordinator in conjunction with other identified critical staff shall investigate the extent and scope of the data breach, including the nature of the information impacted, the length of the exposure and the cause of the breach. An immediate assessment of whether the breach has been addressed and contained shall be made and a plan established with all interested parties, including any critical vendors where further steps are needed to assure the security breach has addressed.

Incident Assessment

Once containment has been verified, the Program Coordinator in conjunction with critical internal and external vendor resources, when needed, should verify the extent and nature of the data breach and personally identifiable customer information that has been compromised including each of the insureds affected, the personal data exposed and the insured's financial institution / branch . An Incident Report shall be produced identifying all insured's whose identifiable customer information which was compromised, segregated by financial institution and branch. The Incident Report shall be provided to the Executive Vice President of Sales and Marketing and the Chief Executive Officer.

External Notice and Communication

Upon receipt of the Incident Report, the Chief Executive Officer together with the Executive Vice President of Sales and Marketing, the Program Director and any other resource identified by the CEO, shall establish a communication plan to notify contracted financial institutions whose box holders have been impacted by the breach. The Company shall coordinate with the financial institutions and obtain approval from each on the form and substance of the notice to be provided to the individual box holders. An assessment shall also be made as to the need for, and the form of, any communication to impacted insured's not associated with a financial institution under contract with the Company.

Remediation and Prevention

In conjunction with the implicated vendor, the Program Coordinator shall identify the cause of the breach, then develop and implement a plan to prevent similar events from occurring. The plan should include objective and quantifiable steps to eliminate the breach. Once implemented, the changes shall be tested and monitored to assure effectiveness against the identified weakness that facilitated the breach. The Company shall obtain a written attestation from the implicated vendor that all steps have been taken per the terms of the plan to prevent further similar breaches. A final report shall then be prepared by the Program Coordinator and delivered to the Chief Executive Officer.

Liability Assessment

The Chief Executive Officer may, in his discretion, involve legal resources at any time during the incident response to provide guidance and direction and assessment of potential legal liability. To the extent a potential liability is identified, the Board of Directors shall be provided notice and given a copy of the final report.