Business Continuity Plan Summary

Our policy is to maintain a comprehensive business continuity plan designed to permit us to resume critical organizational functions that would be necessary in the event of a disaster.

A disaster is defined as a disruption of normal organizational functions where the expected time for returning to normalcy would seriously impact our ability to maintain customer commitments and regulatory compliance through our standard business operations.

RECOVERY AND RESTORATION PROGRAM

Our recovery and restoration program is designed to resume operations and critical systems as quickly as possible, thereby allowing customers to transact business in a secure manner. In addition, we use multiple geographically dispersed data centers equipped with mirroring and replication technologies, allowing for efficient fail-over recovery of critical systems and resumption of business.

REMOTE TECHNOLOGIES

To facilitate recovery, we have implemented technologies (VPN, Citrix, etc.) that allow our employees to resume critical operations by working remotely during a disaster event.

MULTIPLE DATA CENTERS

Critical systems are housed in state-of-the-art, geographically dispersed data centers. Critical systems and data (files, databases, etc.) are mirrored and replicated between data centers. Company sites and data centers are connected by high-speed bandwidth, including Metro Ethernet, MPLS, and VPN technologies.

COMMUNICATION

Redundant phone systems with rerouting technology are located at geographically dispersed data centers to continue telecommunication during a recovery. We also use a third-party interactive voice response ("IVR") solution with a configurable call-forwarding feature, allowing incoming calls to be quickly rerouted. The websites also may be utilized to communicate status updates regarding a disaster event.

ACCESS TO WEBSITE

We use highly available architecture to assure customer access to websites. This includes many redundant web servers in multiple geographically dispersed data centers. We also use internet load balancing and rerouting technology to maintain website availability.

TESTING

Disaster recovery testing is conducted several times each year. Our information technology division employees and testers from our various business units report to a designated location for each test. Employees follow their activation procedures to enable critical technology systems and infrastructure. The testers use predefined, web-based surveys that guide them through business-critical tests. The testers are required to log the results of each test. That information is then used to calculate a grade for the disaster recovery test.