October 1, 2012

Via Electronic Mail

Ms. Elizabeth Murphy
Secretary
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: ***File No. 4-652; Technology and Trading Roundtable***

Dear Ms. Murphy:

TD Ameritrade Holding Corporation[1] ("TD Ameritrade" or "the Company") appreciates the opportunity to participate in the upcoming Technology and Trading Roundtable and submit the following comments. The Company applauds the U.S. Securities and Exchange Commission ("Commission") for organizing this forum to explore the technology risks present in the market today, how to prevent technology-related errors and how to respond to errors and malfunctions in real-time. It is no secret that TD Ameritrade's largely internet-driven business model is highly dependent on its technology systems. As a result, the Company expends significant amounts of effort, both in terms of time and money, focusing on the execution and operational risks inherent in operating predominantly an internet-based business. What follows is an overview of how TD Ameritrade views and, more importantly, manages technology risk.

I. FRAMEWORK

At TD Ameritrade, we think of incidents as having three distinct components. Generally, these are categorized as a *latent defect* or issue, a *trigger*, and an effect (*impact*). A well run system employs a "defense in depth" strategy to layer controls over each of these three components. Not every scenario requires control through the same layers, and the level of layers is determined generally by the extent of the likelihood of the identified issue.

[1] TD Ameritrade Holding Corporation, through its broker-dealer and investment adviser subsidiaries, offers investors and independent registered investment advisors ("RIAs") technology, people and education to help make investing and trading easier to understand and do. Online or over the phone. In a branch or with an independent RIA. First-timer or sophisticated trader. Our clients want to take control, and we help them decide how – bringing Wall Street to Main Street for more than 36 years. TD Ameritrade, Inc. serves an investor base of over 5.7 million funded accounts with approximately $461 billion in assets. During August 2012, TD Ameritrade, Inc. averaged a total of 303,000 client trades per day.

The core of our operational risk analysis revolves around the concept of "materiality." The Company scores every incident of any size (and applies hypothetical scores to potential incidents) based on client impact. In addition, a "likelihood" factor is applied to potential incidents, which captures the probability of its realization. Actual incidents, by definition, are scored with a likelihood of 100% in the period in which they occur.

Materiality encompasses a number of components that are used to measure client impact. These include: (1) number of clients affected; (2) criticality of the system(s) affected; (3) duration of the incident; and (4) time of day (market open hours are weighted differently from afterhours). As part of the analysis, we further consider (a) susceptibility (the likelihood of an occurrence of a latent defect) and (b) exploitability (the likelihood that the environment will trigger the incident).

In general, it has been our experience that controls against *latent defects* tend to be broad or systemic, meaning that a single control can cover a large number of representative cases. Software quality programs, for example, can be effective at preventing a large number of latent code issues. The broad applicability of these controls tends to make them very efficient and desirable.

Trigger controls tend to be less broad and more specific to a type of incident. For example, the controls used to prevent accidental file deletion are different from the controls used to prevent accidental deployment. They can be highly effective for a given scenario, but their narrow applicability makes them less efficient. Scenario planning often focuses on triggers.

Impact mitigation is the last line of defense in controls. At this point, the incident has occurred and the goal is to limit its potential effect. Since so much already has been developed to drive efficiency in incident detection and management, often there are diminishing returns associated with investing in faster detection. Detection controls are a form of insurance, and although they tend to be broadly applied, they are very costly to build or use, making them necessary but not efficient. Their value lies in the fact that they tend to be so broad that they cover a wide range of low likelihood but high impact events, such as inclement weather and environmental disruptions, pandemics, and "black swan" events. Strategies like "kill switches" fall into this category.

II. KILL SWITCHES

In general, TD Ameritrade is wary of the use of systemic kill switches and even less comfortable with the concept of automated kill switches. TD Ameritrade has the ability to cut connectivity in its order routing system should the Company determine that it is necessary. The issue the Company has with systemic switches (which cut all connectivity) is that they effectively shut down business with no chance of recovery within a reasonable period. This may halt the immediate economic harm, but probably increases the reputational harm exponentially. Either can be so impactful that it is likely that there will be strong reluctance to use such an

extreme mitigation strategy. The cost and complexity to build something like a kill switch does not appear justified in light of its limited utility, if any.

Kill switches that are triggered automatically carry more potential harm than manual ones. Any thresholds set based on the above logic will not trigger at arguably appropriate times. In addition, the risk of kill switches accidentally misfiring could cause great harm for no reason (since software is imperfect, this is as likely a scenario as a significant failure). The potentially devastating impact caused by the firing of a kill switch will drive firms to be even more conservative in their thresholds – placing them so high that they become useless.

Selective kill switches that cut connectivity to a specific destination, given multiple options for routing, make more sense. Also, the application of human judgment should not be overlooked in the decision to activate the switch.

III. FAST FAILBACK

"Fast failback" is an important mitigation strategy as it permits a firm to revert quickly to the previously used code if issues develop. For example, fast failback can be achieved by leaving one subset of a data center (or "pod") in environmental isolation from code changes being deployed. If the deployed code fails for some reason, a firm can cut back to the "pod" that has not been upgraded. This notion of "fast failback" enables firms to recover from a technology coding or release miscue without a lengthy debug cycle. While "fast failback" cannot be used in every deployment, it can be used in many scenarios.

IV. CONCLUSION

TD Ameritrade appreciates the opportunity to participate in the Roundtable and to be able to share its thoughts concerning the Commission's review of how firms manage risk. Please feel free to contact me at 201-369-8675 if you have any questions regarding these comments.

Respectfully Submitted,

/s/

Lou Steinberg
Managing Director, Chief Technology Officer
TD Ameritrade