Appendix 2 - Text of Amendments to Dealer Member Rule 3100 (Blackline to reflect non-material changes)

The Dealer Member Rules are hereby amended by adding the following section to Rule 3100:

RULE 3100
REPORTING AND RECORDKEEPING REQUIREMENTS

…

I. B. 1.1 CYBERSECURITY REPORTING

(1) For purposes of this sub-section, a "cybersecurity incident" includes any act to gain unauthorized access to, disrupt or misuse a *Dealer Member's* information system, or information stored on such information system, that has resulted in, or has a reasonable likelihood of resulting in:

(i) substantial harm ~~or inconvenience~~ to any *person*,

(ii) a material impact on any part of the normal operations of the *Dealer Member*,

(iii) invoking the *Dealer Member's* business continuity plan or disaster recovery plan, or

(iv) the *Dealer Member* being required under any applicable laws to provide notice to any government body, securities regulatory authority or other self-regulatory organization.

(2) A *Dealer Member* must report to *the Corporation,* in writing, within 3 calendar days from discovering a c*ybersecurity incident*.

(3) The report provided by the *Dealer Member* to *the Corporation* under subsection (2) must include the following information:

(i) a description of the *cybersecurity incident*,

(ii) the date on which or time period during which the *cybersecurity incident* occurred and the date it was discovered by the *Dealer Member*,

(iii) a preliminary assessment of the *cybersecurity incident*, including the risk of harm ~~or inconvenience~~ to any *person* and/or impact on the operations of the *Dealer Member*,

(iv) a description of immediate incident response steps the *Dealer Member* has taken to mitigate the risk of harm ~~or inconvenience~~ to *persons* and impact on its operations, and

(v) the name of and contact information for an *individual* who can answer, on behalf of the *Dealer Member*, any of *the Corporation's* follow-up questions about the *cybersecurity incident*.

(4) Within 30 days, unless otherwise agreed by the Corporation, from discovering a *cybersecurity incident*, a *Dealer Member* must provide the Corporation with an incident investigation report, in writing, that includes the following information:

(i) a description of the cause of the *cybersecurity incident*,

(ii) an assessment of the scope the *cybersecurity incident*, including the number of *persons* harmed ~~or inconvenienced~~ and the impact on the operations of the *Dealer Member*,

(iii) details of the steps the *Dealer Member* took to mitigate the risk of harm ~~or inconvenience~~ to *persons* and impact on its operations,

(iv) details of the steps the *Dealer Member* took to remediate any harm ~~or inconvenience~~ to any *persons*, and

(~~i~~v) actions the *Dealer Member* has or will take to improve its *cybersecurity incident* preparedness.