

Because of the scope of the proposed amendments and the significant costs to broker-dealers and others (particularly smaller broker-dealers) to comply, we believe that some items need to be clarified so as to minimize the burdens attendant to compliance.

With respect to proposed Section 248.30(a)(3)(iv), we believe that a more objective requirement should replace the concept of “regularly” test or otherwise monitor. Because such testing will be time-consuming and costly, firms should be able to have more specific guidance as to what minimum level of testing is required. Under the current proposed language, a regulator would have no standards and could easily second-guess a firm as to whether testing or otherwise monitoring has been adequately carried out. Additionally, without more specific guidelines, regulatory examinations might result in different conclusions for similar situations.

With respect to the requirement under Section 248.30(a)(4)(v), we agree wholeheartedly that “the proposed notice requirement is intended to avoid notice to the Commission in every case of unauthorized access, and to focus scrutiny on information security breaches that present a greater potential likelihood for harm.” To ensure that this objective is carried out in practice, we believe that, concurrently with the adoption of a final rule, the Commission should issue interpretive notices, questions and answers or other explanatory comment in order to give detailed guidance (including specific examples) to firms to enable them to better determine when there is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience and thereby trigger the notice requirement.