12/12/2016

D E C I S I O N

Nasdaq Clearing Aktiebolag
via the Chairman of the Board of Directors
105 78 Stockholm

FI Ref. 15-9258
Notification no. 1

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Remark and administrative fine

Finansinspektionen's decision (to be announced 13 December 2016 at 8:00 a.m.)

1. Finansinspektionen is issuing Nasdaq Clearing Aktiebolag (556383-9058) a remark.

   (Chapter 25, section 1 of the Securities Market Act [2007:528])

2. Nasdaq Clearing Aktiebolag shall pay an administrative fine of SEK 25,000,000.

   (Chapter 25, section 8 of the Securities Market Act)

To appeal the decision, see *Appendix 1*.

Summary

Nasdaq Clearing Aktiebolag (Nasdaq Clearing or the company) is a Swedish limited liability company that holds authorisation to provide clearing services as a central counterparty in accordance with the provisions set out in Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (EMIR).

Finansinspektionen has investigated how well Nasdaq Clearing has complied with certain fundamental requirements that are placed on a central counterparty in accordance with the provisions set out in EMIR.

The investigation has focused on how the company handles cyber risks. Since, for example, the function for informational security is outsourced to the Group's parent company, Nasdaq, Inc., the company's independence was reviewed during the investigation. Finansinspektionen finds that Nasdaq Clearing has not acquired the information required to assess the quality of the delivered services and place sufficient requirement on the supplier. The investigation also shows that Nasdaq Clearing has not had a sufficient basis in

its risk management to make the decisions that were made and that it has not taken local conditions into consideration. Finally, Finansinspektionen has identified that the company's continuity policy and disaster recovery plan were prepared without considering a scenario that manages the risk of cyber attacks.

Because central counterparties have a systemically important function in the financial system, they are subject to requirements on internal governance and control, risk management and information security that are very strict. Finansinspektionen's investigation shows that Nasdaq Clearing has not fully met these requirements. The deficiencies have been of such a nature that Finansinspektionen judges there to be grounds on which to intervene against Nasdaq Clearing. However, the company's infringements have not been so serious that it is necessary to withdraw its authorisation. Finansinspektionen is therefore issuing the company a remark and an administrative fine of SEK 25 million.

1 Background

1.1 Operations of the company

Nasdaq Clearing Aktiebolag (Nasdaq Clearing or the company) holds authorisation to provide clearing services as a central counterparty in accordance with the provisions set out in Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (EMIR). The company is subject to Finansinspektionen's supervision in accordance with Chapter 23, section 1, first and second paragraphs of the Securities Market Act (2007:528). Nasdaq Clearing reported in 2015 annual net sales of approximately SEK 637 million and 66 employees.

Nasdaq Clearing is part of the Nasdaq Group, an international group with operations in, for example, the USA and the Nordic and Baltic countries. The operations largely consist of operating trading venues for financial instruments.

The Nordic subsidiaries of the Nasdaq Group, including Nasdaq Clearing, have outsourced a large part of their functions to the parent company, Nasdaq, Inc. One of the services the parent company delivers to Nasdaq Clearing is information security.

1.2 The matter

As part of its supervision of Nasdaq Clearing, Finansinspektionen started an investigation in June 2015. Finansinspektionen also conducted the same investigation at the sister company, Nasdaq Stockholm Aktiebolag, which operates the regulated market, Nasdaq Stockholm.

The investigation focused on how the company manages cyber risks, i.e. the risk that the company will be subject to cyber attacks. In this memorandum, "cyber attack" refers to an electronic attack on information systems,

technological infrastructure, computer networks or personal computers. The aim of a cyber attack is normally to gain access to, manipulate or destroy information, or to cause a denial of service. Efforts to prevent cyber attacks are referred to in this memorandum as “cyber security”. The risk analyses that Finansinspektionen has conducted in recent years have identified cyber attacks against financial infrastructure companies as a significant risk, in part because there is a high probability that these companies will be attacked and in part because such attacks can cause extensive damage. A successful cyber attack against an infrastructure company, for example, could lead to the disruption, manipulation or termination of trading for either an extended or a short period of time. Such an event could have a seriously damaging effect on confidence in the financial markets. Therefore, the aim of the investigation was to review the company’s risk management, governance and control in this area.

Finansinspektionen conducted a desk review, which means that the information was obtained via a questionnaire and follow-up requests for more information. This information was supplemented with two onsite visits. The first focused on the company’s technological controls, while the second focused on the company’s risk management and governance and control.

On 25 January 2016, Finansinspektionen sent a verification letter to Nasdaq Clearing. In this letter, Finansinspektionen outlined in detail its observations from the investigation. On 16 February 2016, the company submitted its response to the verification letter.

Nasdaq Clearing was given the opportunity to respond to Finansinspektionen’s preliminary assessment that the company had disregarded its obligations. On 7 July 2016, Nasdaq Clearing submitted a response to Finansinspektionen. On 26 August, Nasdaq Clearing visited Finansinspektionen and submitted information verbally.

2 Applicable provisions

Central counterparties fulfil a systemically important function in the financial system and they are therefore subject to organisational requirements that are quite high. The fundamental requirements governing the operations of central counterparties are set out in EMIR. There are also more detailed requirements set out in Commission Delegated Regulation (EU) No 153/2013 of 19 December 2012 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on requirements for central counterparties (Commission Delegated Regulation (EU) No 153/2013). The delegated regulation contains regulations regarding, for example, governance arrangements, risk management, IT systems and business continuity.

Various provisions in the regulations emphasise the importance of central counterparties’ independence in relation to, for example, service providers and companies that are part of the same group. Provisions in EMIR state that, when outsourcing, a central counterparty shall remain fully responsible for

discharging all of its obligations under EMIR and that the outsourcing may not result in the delegation of responsibility. There are also provisions specifying the minimum number of independent Board members and the procedures for ensuring that the interests of the clearing members and clients are not disregarded. For example, Commission Regulation (EU) No 153/2013 contains provisions regarding a central counterparty's independence in relation to a group to which it belongs. Central counterparties that are part of a group shall take into account any implications of the group for their governance arrangements, for example if they are sufficiently independent to be able to meet their statutory obligations as a separate legal person and if their independence may be compromised by the group structure.

For a description of the applicable provisions, *see Appendix* 2.

3 Finansinspektionen's assessment

In this section, Finansinspektionen accounts for its observations and assessments with regard to how Nasdaq Clearing complies with certain provisions that govern the operations of central counterparties. The focus is on deficiencies in the company's outsourcing of services as well as its risk management and plans for business continuity.

3.1 Outsourcing

Central counterparties are allowed to outsource operational functions, i.e. reach an agreement that a third party will carry out certain activities, but outsourcing is carefully regulated in order not to compromise the central counterparty's independence and systemically important function on the financial market.

Article 35(1) of EMIR states that where a central counterparty outsources operational functions, services or activities, it shall remain fully responsible for discharging all of its obligations under EMIR. Article 35(1)(a) of EMIR states that the central counterparty shall ensure that the outsourcing does not result in the delegation of responsibility. Article 35(1)(g) of EMIR also states that, when outsourcing, the central counterparty shall retain the necessary expertise and resources to evaluate the quality of the services provided and the organisational and capital adequacy of the service provider and to supervise the outsourced functions effectively and manage the risks associated with the outsourcing. The central counterparty shall also supervise these functions and manage these risks on an ongoing basis. According to Article 35(1)(h), the central counterparty shall have direct access to relevant information about the outsourced functions.

Article 4(4) of Commission Regulation (EU) No 153/2013 prescribes that the governance arrangements shall ensure that the board of a central counterparty assumes final responsibility and accountability for managing the central counterparty's risks. The board shall define, determine and document an appropriate level of risk tolerance and risk bearing capacity for the central counterparty. The board and senior management shall ensure that the central counterparty's policies, procedures and controls are consistent with the central

counterparty's risk tolerance and risk bearing capacity, and they shall address how to identify, report, monitor and manage risks.

As previously mentioned, Nasdaq Clearing has outsourced a number of services to the Group's parent company Nasdaq, Inc. The outsourced services include information security, which in turn includes cyber security.

At the time of the investigation, there was a general main agreement between the parties for all services that Nasdaq Clearing had outsourced to the Group's parent company. However, this agreement did not contain any detailed descriptions of the relevant services or established Service Level Agreements (SLA). The main agreement did have some appendices that contained brief descriptions of the services, but there were no detailed quality measures, even though the company's own outsourcing policy states that the precise requirements must be specified in the SLA.[1]

Nasdaq Clearing has not received any continuous information or follow-up statistics that provide an overview of the service delivery. At the time of the investigation, there was no ongoing follow-up of the agreement and the delivery.

Furthermore, the company has not had access to information about threats, personnel situations, incident management, ongoing projects or training in cyber security. Neither has there been any information about threats related to Sweden or the Nordic region.

In its response, Nasdaq Clearing states that the company considers that the main agreement already at the time of the investigation met the legal and business requirements that can be placed on such an agreement, with the exception that there was no SLA. The company also states that the main agreement has now been supplemented with an SLA. Furthermore, Nasdaq Clearing states that its CTO is responsible for all outsourcing of technology, including supervision of agreements and follow-up of service delivery. The CTO provides the company's Board of Directors with reports within the CTO's area of responsibility.

Nasdaq Clearing makes the statement in its response that the company believes that both the role of the CTO and the people who have held this role in the company have fulfilled the requirements set out in EMIR with regard to expertise as the orderer of a service. According to the company, there is thus sufficient expertise for evaluating the delivered services. In its statement, Nasdaq Clearing also states that both the company's management and important forums, such as the Local Risk Management Forum, have received regular reports regarding the follow-up of the service delivery. This has given the company direct access to relevant information about the outsourced

[1] "...the precise requirements concerning the performance of the service provider should be specified and documented by a service level agreement, taking account of the objective of the outsourcing solution."

functions, in the opinion of Nasdaq Clearing. The company also points to the fact that the company's management team and Board of Directors have received follow-up reports through the annual overview of, for example, the main agreement. Nasdaq Clearing also takes the position in its response that incident-related reporting is conducted weekly, daily or when an incident occurs based on a pre-determined structure. If incidents are critical in nature, the continuity and disaster recovery plans enter into force and relevant stakeholders are informed.

Finansinspektionen notes that Nasdaq Clearing takes the position that regular reports have been submitted and to demonstrate this provided an overview of the reporting procedures prepared by the company's CTO. However, there are no minutes or other documentation included among the documents the company attached to its response that show proof of any actual reporting from the time before the investigation. Neither is there any documentation that shows that the Board of Directors in any other way has ensured that the company has had direct access on an ongoing basis to relevant information about the outsourced operational functions. Finansinspektionen therefore makes the assessment that Nasdaq Clearing has not fulfilled the requirements set out in Article 35(1)(h) of EMIR.

The documents that Nasdaq Clearing attached to its response also do not include anything showing that the company has carried out documented follow-up of the delivered services. The company has referred to a presentation and minutes for a review of the main agreement, but this review occurred after the investigation was started. These documents also do not contain any actual follow-up of the delivery of information security services, but rather contain a brief description of the services and some new information from the service provider in a bullet point list.

Because there has been no SLA for the information security services, neither has there been in practice any possibility for the company to conduct any detailed follow-up. It is Finansinspektionen's opinion that effective monitoring of outsourced operational functions as a minimum requires regular follow-up of the delivery and the agreement.

The investigation also shows that the Board of Directors has not had access to any information about threats and risks in conjunction with the outsourcing. The Board of Directors has also not had sufficient information for managing the risks that arose from the outsourcing of information security. Neither has the Board of Directors faced conditions for managing the outsourcing risks.

In order to be able to evaluate the quality of the provided services and monitor the outsourced functions, the central counterparty must have the necessary resources and expertise. Nasdaq Clearing has not documented any follow up of the delivery. This means that Nasdaq Clearing has not had the possibility to monitor the outsourced functions or manage the risks arising from the outsourcing on a regular basis. Nasdaq Clearing has therefore not met the requirements for outsourcing as set out in Article 35(1)(g) in EMIR.

The above-mentioned deficiencies combined with the fact that the company has not ensured that there was an SLA in place to enable a critical evaluation of the delivery are an indication in Finansinspektionen's opinion that the company to a large extent has relied on the service provider's expertise.

Finansinspektionen therefore makes the assessment that Nasdaq Clearing, with regard to cyber security, has delegated in practice its responsibility to the service provider and that the outsourcing has not occurred in compliance with Article 35(1)(a) of EMIR. The company's Board of Directors has also not taken responsibility for the management of the company's risks. As a result, the outsourcing has therefore led to Nasdaq Clearing being non-compliant with Article 4(4) of Commission Regulation (EU) No. 153/2013.

3.2 Risk management

One of the fundamental requirements that is placed on a central counterparty is that it shall have effective processes to identify, manage, monitor and report the risks to which it is or might be exposed. This is set out in Article 26(1) of EMIR.

The requirement on risk management is set out in Article 4 of Commission Regulation (EU) No 153/2013. According to Article 4(1), central counterparties shall have a sound framework for the comprehensive management of all material risks to which they are or may be exposed. They shall establish documented policies, procedures and systems that identify, measure, monitor and manage such risks. In Article 4(2), central counterparties shall take an integrated and comprehensive view of all relevant risks, including the risks they bear from and pose to their clearing members and, to the extent practicable, clients and other entities. Article 4(3) states that central counterparties shall develop appropriate risk management tools to be in a position to manage and report on all relevant risks.

According to Article 4(4), the governance arrangements shall ensure that the board of a central counterparty assumes final responsibility and accountability for managing the central counterparty's risks. The board shall define, determine and document an appropriate level of risk tolerance and risk bearing capacity for the central counterparty. The board and senior management shall ensure that the central counterparty's policies, procedures and controls are consistent with its risk tolerance and risk bearing capacity and that they address how it shall identify, report, monitor and manage risks.

Article 35(1)(e) of EMIR states that outsourcing may not result in depriving the central counterparty from the necessary systems and controls to manage the risks it faces. In the event a central counterparty is part of a group, Article 3(4) of Commission Regulation (EU) No 153/2013 states that the company shall take into account any implications of the group for its own governance arrangements including whether it has the necessary level of independence to meet its regulatory obligations as a distinct legal person.

3.2.1 Deficiencies in risk management

As described previously, large parts of the operational functions are outsourced within the Group and decisions about cyber security are largely made by the parent company, which is also the service provider, and informational considerations are made by global risk management bodies. Given this background, it is important to consider a local risk perspective and provide the global body with information that is relevant from both a local perspective and the perspective of the company. The information that the company submitted with regard to its decision procedure in the area of cyber security at the time of the investigation did not indicate any reporting between the local risk management forum and the parent company's risk management body, Technology Risk Committee. This means that there has been no local risk perspective.

Finansinspektionen has furthermore identified that the company has not had risk management tools for cyber risks that could have provided it with an overview for the assessment of these risks. At the time of the investigation, there was a tool for managing risks, but it did not include cyber risks. Parts of the risk information were available at various units at the parent company, but there was no comprehensive overview of risks related to cyber security, vulnerabilities and problems upon which the information security department and other units, where necessary, were able to draw.

Nasdaq Clearing states in its response that the risk management tool that was previously used (in 2013 and 2014) was temporarily discontinued in respect of the risk self-assessment process. However, the company takes the position that this does not mean that there was no risk reporting. Reporting and follow-up was conducted instead in Excel at the various functions within the organisation. According to the company, the risk management tool will once again be put into service and used for self-evaluation of information security risks.

Finansinspektionen's investigation shows that Nasdaq Clearing did not ensure that the company's local risk perspective was taken into account with regard to cyber security. Neither has Nasdaq Clearing had a comprehensive overview of the threats in this area nor the possibility of producing a relevant overview of the threats for Sweden or the Nordic region. The investigation also shows that the company has not had appropriate tools for managing and reporting on cyber risks. The investigation shows that there is a risk management tool, but it is clear from the investigation that this tool to date has not been used to manage cyber risks.

Finansinspektionen makes the assessment that the company has not fully discharged the requirement on effective processes to identify, manage, monitor and report risks in accordance with Article 26(1) of EMIR. Neither has Nasdaq Clearing had a sound system for the comprehensive management of all risks in accordance with Article 4(1) of Commission Regulation (EU) No 153/2013.

The company has also had neither an integrated and comprehensive view of cyber risks nor appropriate risk management tools to be in a position to manage and report on these risks. Nasdaq Clearing has also not sufficiently taken into account the implications of the Group for the company's own governance arrangements. The question may therefore be raised whether the company has the necessary level of independence to meet its regulatory obligations as a distinct legal person. Finansinspektionen therefore makes the assessment that Nasdaq Clearing has also not met the requirements set out in Articles 3(4), 4(2) and 4(3) of Commission Regulation (EU) No. 153/2013.

3.2.2 Deficiencies in the Board of Director's establishment of risk tolerance and risk bearing capacity with regard to cyber risks

The investigation shows that Nasdaq Clearing's Board of Directors has not made independent decisions regarding the risk tolerance level and risk bearing capacity for the company with regard to cyber risks. The Board has neither had access to any continuous reporting about cyber security from the service provider nor access to any of its own information that could have served as a basis for such decisions. The information submitted by Nasdaq Clearing shows that the Board has approved the policy for information security that the parent company, which is also the service provider, prepared for the Group. According to the company, this policy has served as a basis for a level of risk tolerance concerning information security that was approved by the parent company's audit committee in August 2015. However, it has not been shown that Nasdaq Clearing at the time of the investigation made any independent decisions regarding the risk tolerance level and risk bearing capacity.

Finansinspektionen also noted that Nasdaq Clearing has not had a process for linking its risk tolerance level and risk bearing capacity to its financial considerations.

Nasdaq Clearing states in its response that the company's Board of Directors decided on risk appetite and risk tolerance in May 2016.

Finansinspektionen notes that the Board of Directors of Nasdaq Clearing at the time of the investigation had not defined, determined and documented the central counterparty's appropriate risk tolerance level and risk bearing capacity with regard to cyber risks. The Board and senior management therefore have not been able to ensure that the company's policies, procedures and controls are consistent with its risk tolerance and risk bearing capacity. Finansinspektionen therefore makes the assessment that Nasdaq Clearing has not met the requirements set out in Article 4(4) of Commission Regulation (EU) No 153/2013.

An important part of risk control is determining the economic consequences that will result from various positions with regard to risk tolerance levels and risk bearing capacity. The investigation shows that Nasdaq Clearing has not had a process for linking decisions about its risk tolerance level and risk bearing capacity to financial considerations. As a result, there have not been

any clear rules for how a change in the threat profile affects the investments in cyber security that are needed. The Group's risk management strategies have thus not been anchored in the company's financial plans, which could result in Nasdaq Clearing not having financial contingencies for managing the risks. Finansinspektionen therefore makes the assessment that cyber risks have not been subject to a sound system for risk management in accordance with Article 4(1) of Commission Regulation (EU) No 153/2013.

3.2.3 Deficiencies in risk management in collaborations that require technological contacts

Nasdaq Clearing has technological contact with a number of other parties in addition to the parent company. "Technological contact" refers to contact that entails that the company's IT system in some way interacts with the other party's IT system or in any other way allows the other party access to the company's own IT system. Finansinspektionen notes that requirements on including conditions related to cyber security in agreements were only present in agreements with suppliers. In terms of collaboration with other parties with which the company has technological contact, the company has not had any insight into cyber security and there has not been any exchange of information about threats and incidents between the company and these parties, either.

Nasdaq Clearing's response states that the Group is working to establish a global process for managing counterparty risks related to information security.

Finansinspektionen makes the assessment that the absence of insight into the cyber security of the parties with which Nasdaq Clearing has technological contact could lead to the risks presented by these technological contacts not being considered and managed in a satisfactory manner. There is also a risk that the company is more vulnerable in its relationship with its partners since it cannot ensure that they have established a standard for managing cyber risks. Nasdaq Clearing may also be missing out on valuable information about potential threats.

Because there has not been any exchange of information regarding relevant cyber risks between Nasdaq Clearing and other parties with which the company has technological contact, Finansinspektionen makes the assessment that Nasdaq Clearing in this respect does not have an integrated and comprehensive view of relevant risks and that the company thereby does not fulfil the requirements set out in Article 4(2) of Commission Regulation (EU) No 153/2013.

3.3 Business continuity

Article 34(1) of EMIR states that a central counterparty shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan aiming at ensuring the preservation of its functions, the timely recovery of operations and the fulfilment of the central counterparty's obligations. Such a plan shall at least allow for the recovery of all transactions

at the time of disruption to allow the central counterparty to continue to operate with certainty and so the central counterparty is able to complete settlement on the scheduled date.

According to Article 17(4) of Commission Regulation (EU) No 153/2013, the business continuity policy and disaster recovery plan shall ensure a minimum service level of critical functions. Furthermore, according to Article 17(5) of the same regulation, the disaster recovery plan shall include recovery point objectives and recovery time objectives for critical functions and determine the most suitable recovery strategy for each of these functions. Article 17(6) states that the business continuity policy shall identify the maximum acceptable time for which critical functions and systems may be unusable. The maximum recovery time for critical functions that must be included in the policy may not be longer than two hours.

In conjunction with the business impact analysis that shall be conducted in accordance with Article 18 of Commission Regulation (EU) No 153/2013, the central counterparties, in accordance with Article 18(2), shall analyse how various scenarios affect the risks to critical business functions.

With regard to disaster recovery, central counterparties, in accordance with Article 19(1) of Commission Regulation (EU) No 153/2013, shall have in place arrangements to ensure continuity of their critical functions based on disaster scenarios. These arrangements shall at least address the availability of adequate human resources, the maximum downtime of critical functions and fail over and recovery to a secondary site.

According to the information provided by Nasdaq Clearing, cyber attacks were not included in the company's scenario-based risk analysis at the time of the investigation, and the company has therefore not established how these scenarios in particular affect the risks for its critical business functions or IT systems. Neither were there any preparations for alternative arrangements or documentation of tested scenarios to ensure that Nasdaq Clearing would be able to recover critical functions or IT systems in a timely manner.

Nasdaq Clearing has not been able to specify how it will be able to manage events in which IT systems are attacked or information is manipulated or corrupted. Nasdaq Clearing states in its response that the scenarios that include cyber attacks have been implied in the company's continuity plans, but that no scenarios expressly for cyber attacks have been included. The company is now taking measures to include such scenarios in its continuity plans.

In Finansinspektionen's view, scenario-based analyses and arrangements cannot function for implied scenarios since each scenario may require a unique series of measures. There is no guarantee that a disaster scenario entailing the manipulation or corruption of data due to a cyber attack can be managed using the same arrangements as other disaster scenarios.

Scenarios related to cyber attacks have not been included in the scenario-based risk analysis that must be used according to Article 18(2), or among the disaster scenarios that served as a basis for the continuity arrangements according to Article 19(1) of Commission Regulation (EU) No 153/2013. Nasdaq Clearing therefore has not had sufficient analysis and planned measures to be able to maintain its data authenticity and protect its data integrity in situations where information has been manipulated or corrupted.

There has therefore been a risk that Nasdaq Clearing would not be prepared to be able to recover critical functions within the time limit specified in the continuity policy in accordance with the requirements set out in Article 17(6) of the Regulation. Nasdaq Clearing has not conducted any type of analysis of the most appropriate recovery strategy with regard to cyber-related scenarios as described in Article 17(5) of the Regulation. In summary, at the time of the investigation, there was inadequate preparation for cyber attacks or deficient data integrity in the company's contingency planning. Finansinspektionen therefore makes the assessment that Nasdaq Clearing does not meet the requirements set out in Articles 17(4)–17(6), 18(2) and 19(1) of Commission Regulation (EU) No 153/2013.

4 Consideration of intervention

4.1 Applicable provisions

Chapter 1, section 1, third paragraph of the Securities Market Act states which rules in the act apply to the clearing operations of central counterparties. These include the provisions set out in Chapter 25, sections 1, 2, 6 and 8–10 regarding interventions.

According to Chapter 25, section 1, first paragraph of the Securities Market Act, Finansinspektionen shall intervene, for example, where a Swedish clearing organisation has breached its obligations pursuant to the law, other regulations that govern the company's operations, the company's articles of association, statutes or rules or internal instructions which are based on a legislation that governs the company's operations.

According to the section's second paragraph, Finansinspektionen shall then issue an order to, within a specific time, limit or reduce the risks in the business in some respect, limit or preclude in full payment of dividends or interest or take another measure to rectify the situation, issue an injunction against executing resolutions or issue a remark. Where the infringement is serious, the authorisation of the company shall be withdrawn or, if sufficient, a warning issued.

Chapter 25, section 1b, first paragraph of the Securities Market Act states that when determining the sanction, Finansinspektionen shall take into consideration the gravity of the infringement and its duration. Special consideration shall be given to the nature of the infringement, the tangible and

potential effects of the infringement on the financial system, the losses incurred and the degree of responsibility.

According to Chapter 25, section 1c, first paragraph of the Securities Market Act, in addition to that set out in section 1b, as an aggravating circumstance, consideration shall be given to previous infringement by the company. In conjunction with this determination, particular weight should be attached to whether the infringements are similar in nature and the time which has elapsed between the various infringements. According to the second paragraph of the same section, mitigating circumstances may be considered where

1. the company to a significant extent, through active cooperation, facilitated Finansinspektionen's investigation, and
2. the company promptly ceased the infringement after it was reported to, or identified by Finansinspektionen.

According to Chapter 25, section 2 of the Securities Market Act, Finansinspektionen may refrain from intervention pursuant to section 1 where a violation is insignificant or excusable, where the company makes rectification, or where any other body has taken measures against the company which are deemed sufficient.

Chapter 25, section 8, first paragraph of the Securities Market Act states that where a Swedish securities institution, a stock exchange or a Swedish clearing organisation has been notified of a decision regarding a remark or warning pursuant to section 1 of the same chapter, Finansinspektionen may decide that the company must pay an administrative fine.

According to Chapter 25, section 9, first paragraph of the Securities Market Act, the administrative fine for a Swedish securities institution, a stock exchange or a Swedish clearing organisations shall be set at an amount not to exceed

1. ten per cent of the company's net sales during the immediately preceding financial year,
2. two times the profit which the company realised as a result of the regulatory infringement, where the amount can be ascertained, or
3. two times the costs which the company avoided as a result of the regulatory infringement, where the amount can be ascertained.

The preparatory works for the provision state that it is the highest amount of the alternative calculations that constitutes the maximum fine (Bill 2013/14:228 p. 235).

The second paragraph of the same section states that the administrative fine may not be set at less than SEK 5,000.

Once the size of the administrative fine is determined, according to Chapter 25, section 10 of the Securities Market Act, special consideration shall be given to

such circumstances as those set out in sections 1b and 1c, the company's financial position and the profit the company realised as a result of the regulatory infringement or the costs which were avoided, if such can be ascertained.

4.2 Response of the company

In its response, Nasdaq Clearing states in part the following with regard to a possible intervention by Finansinspektionen.

Nasdaq Clearing believes that the deficiencies that Finansinspektionen highlights in its investigation, when placed against a background of Nasdaq Clearing's security level as a whole, the complexity of and rapid changes in the area and the general lack of clear guidance in laws, regulations and recommendations, neither have introduced significant risks nor can be viewed as systemically critical.

Nasdaq Clearing further states that the company has consistently implemented improvements to rectify deficiencies. Since Finansinspektionen opened its investigation, Nasdaq Clearing has treated the authority's observations and preliminary assessment with the utmost seriousness, and the company immediately started its own project to enhance and improve cyber security. Since February 2016, Nasdaq Clearing has worked in accordance with an action plan to improve cyber security within the organisation. The action plan is linked to the observations that Finansinspektionen made during its investigation and contains, for example, a status for every action. This will be approved by the Board and discussed on a quarterly basis by the Board in the future. Nasdaq Clearing also points out that the improvements also include areas where the company believes it meets the legal requirements since the company is striving to fulfil the requirements as Finansinspektionen believes them to apply.

Nasdaq Clearing further highlights that the company has cooperated with Finansinspektionen, for example through the participation of management in meetings with short notice, by answering questions quickly and through the arrangement of onsite visits with attendance by personnel from Nasdaq, Inc. as requested. The company takes the position that it has thus facilitated Finansinspektionen's investigation.

The company also states that it has made every effort to be in full compliance with the rules in an area that is legally complex and has a regulatory framework that rests on general provisions. The lack of detailed provisions has meant that one of the company's challenges has been the risk of incorrectly interpreting applicable regulation. The definition of "cyber security" also changes on a continuous basis. The company therefore requests that Finansinspektionen take into consideration that the rules on cyber security, in the opinion of the company, are a "moving target" within an area that is undergoing rapid change. Nasdaq believes that the deficiencies that the authority has found should be interpreted against a background of this development and adds that it has not

been fully possible for the company to foresee how the current regulations will be applied and interpreted or which benchmarks would apply.

Finally, Nasdaq Clearing points out that the deficiencies have not caused any damage to the company's systems or operations or any other parties, and neither have they introduced risks for the financial system.

4.3 Assessment of the infringements and choice of intervention

The lack of insight into the trading of OTC derivatives and the occurrence of large counterparty risks that had not be offset by sufficient collateral, combined with a large concentration of risks, are what are believed to have amplified the financial crisis in the autumn of 2008. The implementation of EMIR regulated in part the trading of derivatives in that all standardised OTC derivatives must be cleared through a central counterparty. The central counterparty's assignment is to step in between parties that sign an OTC contract and act as a "buyer for every seller and seller to every buyer", thus guaranteeing the terms in the transaction even if one of the original parties does not fulfil its commitments. The central counterparty thus decreases the operational, legal and marketing risks for the parties on both sides of the transaction. The aim of the regulation has been to increase transparency and control of risks associated with the trading of derivative contracts.

The provisions set out in EMIR aim, for example, to gather, provide an overview of and control counterparty risks, and therefore the requirements that are placed on a central counterparty's management and control of risks are very high. Because there is a statutory requirement on central counterparty clearing for OTC derivatives, the central counterparty also fulfils a critical function for the financial markets. A central counterparty therefore is considered to be a systemically important company.

This means that the organisational requirements that are placed on a central counterparty are particularly high. A number of different provisions in the regulations emphasise the importance of central counterparties' independence with regard to, for example, suppliers and owners. The abundance of rules that aim to ensure the independence of central counterparties shows that the requirements on a central counterparty's independence in relation to, for example, a group to which it belongs, are very high. It is with this starting point that Finansinspektionen has made its assessment regarding the infringements in this matter.

Finansinspektionen's investigation shows that Nasdaq Clearing has not fulfilled all of the requirements that are placed on a central counterparty according to EMIR and Commission Regulation (EU) No 153/2013.

The company has not ensured governance and control when outsourcing services, and neither has it had access to the information that is required for the company's Board of Directors to be able to take full responsibility for these functions. Governance, control and responsibility have instead to a large extent

in practice been transferred to the company's parent company, Nasdaq, Inc. With regard to Nasdaq Clearing, Finansinspektionen takes the position that the company's Board of Directors has not executed the actual governance and control of the company. Finansinspektionen considers this to be a serious deficiency. There were also deficiencies in Nasdaq Clearing's risk management and risk control at the time of the investigation.

The deficiencies have been of such a nature that Finansinspektionen makes the assessment that there are grounds on which to intervene against Nasdaq Clearing in accordance with Chapter 25, section 1 of the Securities Market Act. The company's infringement cannot be considered to be insignificant and no reasons have come to light to treat the infringements as excusable, either. However, the infringements are not so serious that it is necessary to withdraw the company's authorisation. Finansinspektionen is therefore issuing Nasdaq Clearing a remark.

When a company has been issued a remark, Finansinspektionen, in accordance with Chapter 25, section 8 of the Securities Market Act, may also decide on whether the company shall pay an administrative fine. Finansinspektionen makes the assessment that Nasdaq Clearing's infringements have been of such a nature that the remark will be accompanied by an administrative fine.

Finansinspektionen takes the position that it is not possible to determine the extent to which the company realised profits or avoided costs as a result of the infringements. The fine that Nasdaq Clearing shall pay will therefore be set at no more than ten per cent of the company's net sales in the most recent financial year according to Chapter 25, section 9, first paragraph, line 1 of the Securities Market Act. Nasdaq Clearing's net sales for the most recent financial year amounted to approximately SEK 637 million. Finansinspektionen may therefore decide on an administrative fine that may be at the most SEK 63.7 million. The administrative fine may not be set at an amount smaller than SEK 5,000.

The provision regulating how large an administrative fine may be was given its current wording in conjunction with the introduction of the Capital Requirements Directive[2] into Swedish law (see Bill 2013/14:228 p. 235 ff.). Recital (36) of the Capital Requirements Directive states that administrative fines shall achieve a level that is sufficiently high to offset the benefits that an infringement has generated and sufficiently large to be dissuasive even to larger institutions to infringe upon the regulations.

The administrative fine can be seen as a gradation of the infringements. Taking into consideration the content of Recital (36) to the Capital Requirements Directive, Finansinspektionen considers that a starting point for this gradation should be how large the maximum administrative fine may be, rather than to

[2] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

what amount this fine should be set. This means that the administrative fines for two companies that have had similar infringements will not necessarily be set at the same amount if their maximum administrative fines differ, for example because their net sales differ.

When determining the size of the administrative fine, consideration shall be given to the gravity of the infringement and its duration. Special consideration shall be given to the nature of the infringement, the tangible and potential effects of the infringement on the financial system, the losses incurred and the degree of responsibility. Finansinspektionen takes the position that the infringements have not resulted in any losses or tangible effects, but judges the potential effects on the financial system and confidence in the financial market to have been considerable. Central counterparties' critical importance for trading in derivatives plays an important role in setting the administrative fine. This is dependent on how large the potential effects of the infringements in question could be on the financial system. On the other hand, Finansinspektionen, as mitigating circumstance, shall consider if the company to a significant extent, through active cooperation, facilitated Finansinspektionen's investigation and if the company promptly ceased the infringement after it was reported to or identified by Finansinspektionen.

Nasdaq Clearing has presented a comprehensive plan for rectifying many of the deficiencies that have been identified. Finansinspektionen considers this action plan and the improvements that the company has already made to have created adequate conditions for the company to rectify the identified deficiencies in its continuity planning and several of the deficiencies in the company's work with risks. This should to some extent be considered a mitigating circumstance. However, Finansinspektionen makes the assessment that Nasdaq Clearing's change project has not sufficiently focused on clarifying the company's independence in relation to the Group.

In its statement Nasdaq Clearing also took the position that it had facilitated the investigation by cooperating with Finansinspektionen. As stated previously, Finansinspektionen shall take into consideration whether the company significantly facilitated the investigation through active cooperation. According to the preparatory works (Bill 2013/14:228 p. 241), this assumes that the company on its own initiative provides important information that Finansinspektionen itself does not already have at its disposal or can easily find. It is Finansinspektionen's opinion that the company's cooperation has not been more active than what is reasonably expected from a company that is under supervision. This should therefore not be considered a mitigating circumstance.

After a comprehensive assessment of the circumstances that Finansinspektionen shall take into consideration when determining the administrative fine, Finansinspektionen decides that Nasdaq Clearing shall pay an administrative fine of SEK 25 million.

The administrative fine shall accrue to the Government and is invoiced by Finansinspektionen after the decision enters into force.

FINANSINSPEKTIONEN

Sven-Erik Österberg
Chairman of the Board of Directors

Carl Sehlin
Legal Counsellor

A decision in this matter was made by the Board of Directors of Finansinspektionen (Sven-Erik Österberg, Chair, Maria Bredberg Pettersson, Sonja Daltung, Marianne Eliason, Anders Kvist, Astri Muren, Hans Nyman and Gustaf Sjöberg) following a presentation by Legal Counsellor Carl Sehlin. Senior Advisor Per Håkansson, Executive Director Sophie Degenne, Department Director Marie Jesperson, Head of Division Charlotta Tajthy and Senior Legal Counsellor Denny Sternad have participated in the final proceedings.

Appendices
Appendix 1 – How to appeal
Appendix 2 – Applicable provisions

Copy: Nasdaq Clearing Aktiebolag's CEO

N O T I F I C A T I O N R E C E I P T

FI Ref. 15-9258
Notification no. 1

Remark and administrative fine

Document:

Decision regarding a remark and administrative fine for Nasdaq Clearing Aktiebolag announced **on 13 December 2016**

I have received the document on this date.

DATE	SIGNATURE
	NAME IN BLOCK CAPITALS
	NEW ADDRESS (IF APPLICABLE)

This receipt shall be returned to Finansinspektionen **immediately**. If the receipt is not returned, the notification may be issued in another manner, e.g. via a court officer.

If you use the enclosed envelope, there is no charge for returning the receipt.

Do not forget to **specify the date** of receipt.

How to appeal

It is possible to appeal the decision if you consider it to be erroneous by writing to the Administrative Court. Address the appeal to the Administrative Court in Stockholm, but send or submit the appeal to Finansinspektionen, Box 7821, 103 97 Stockholm.

Specify the following in the appeal:

- Name and address
- The decision you are appealing against and the case number
- Why you consider the decision is incorrect
- What change you would like and why you believe the decision should be changed.

Remember to sign the letter.

The appeal must be received by Finansinspektionen within three weeks from the day you have received the decision.

Finansinspektionen will forward your appeal to the Administrative Court in Stockholm, if it has been received on time and Finansinspektionen does not itself change its decision in the manner you have requested.

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 787 80 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Appendix 2

Applicable provisions

Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (EMIR)

Organisational requirements

According to Article 26(1) of EMIR, a central counterparty shall have robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which it is or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures.

Business continuity

Article 34(1) states that a central counterparty shall establish, implement and maintain an adequate business continuity policy and disaster recovery plan aiming at ensuring the preservation of its functions, the timely recovery of operations and the fulfilment of the central counterparty's obligations. Such a plan shall at least allow for the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.

Outsourcing

Article 35(1) states, in part, that where a central counterparty outsources operational functions, services or activities, it shall remain fully responsible for discharging all of its obligations under EMIR.

According to Article 35(1)(a), outsourcing may not result in the delegation of responsibility.

Article 35(1)(g) states that, when outsourcing, the central counterparty shall ensure that it retains the necessary expertise and resources to evaluate the quality of the services provided and the organisational and capital adequacy of the service provider, and to supervise the outsourced functions effectively and manage the risks associated with the outsourcing and supervises those functions and manages those risks on an ongoing basis.

According to Article 35(1)(h), the central counterparty shall have direct access to the relevant information of the outsourced functions.

Appendix 2

Commission Delegated Regulation (EU) No 153/2013 of 19 December 2012 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on requirements for central counterparties (Commission Regulation (EU) No 153/2013)

Governance arrangements

According to Article 3(4) of Commission Regulation (EU) No 153/2013, central counterparties that are part of a group shall take into account any implications of the group for their own governance arrangements including whether they have the necessary level of independence to meet their regulatory obligations as distinct legal persons and whether their independence could be compromised by the group structure or by any board member also being a member of the board of other entities of the same group. In particular, such central counterparties shall consider specific procedures for preventing and managing conflicts of interest including with respect to outsourcing arrangements.

Risk management and internal control mechanisms

According to Article 4(1), central counterparties shall have a sound framework for the comprehensive management of all material risks to which they are or may be exposed. Central counterparties shall establish documented policies, procedures and systems that identify, measure, monitor and manage such risks. In establishing risk-management policies, procedures and systems, central counterparties shall structure them in a way as to ensure that clearing members properly manage and contain the risks they pose to these central counterparties.

Article 4(2) states that central counterparties shall take an integrated and comprehensive view of all relevant risks. These shall include the risks they bear from and pose to their clearing members and, to the extent practicable, clients as well as the risks they bear from and pose to other entities such as, but not limited to interoperable central counterparties, securities settlement and payment systems, settlement banks, liquidity providers, central securities depositories, trading venues served by the central counterparty and other critical service providers.

Article 4(3) of Commission Regulation (EU) No 153/2013 states in part that the central counterparty shall develop appropriate risk management tools to be in a position to manage and report on all relevant risks.

According to Article 4(4), the governance arrangements shall ensure that the board of a central counterparty assumes final responsibility and accountability for managing the central counterparty's risks. The board shall define, determine and document an appropriate level of risk tolerance and risk bearing capacity for the central counterparty. The board and senior management shall

ensure that the central counterparty's policies, procedures and controls are consistent with the central counterparty's risk tolerance and risk bearing capacity, and they shall address how to identify, report, monitor and manage risks.

Business continuity

According to Article 17(4), the business continuity policy and disaster recovery plan shall ensure a minimum service level of critical functions.

Article 17(5) states that the disaster recovery plan shall include recovery point objectives and recovery time objectives for critical functions and determine the most suitable recovery strategy for each of these functions. Such arrangements shall be designed to ensure that in extreme scenarios critical functions are completed on time and that agreed service levels are met.

Article 17(6) states that the business continuity policy shall identify the maximum acceptable time for which critical functions and systems may be unusable. The maximum recovery time for critical functions that must be included in the policy may not be longer than two hours. End of day procedures and payments shall be completed on the required time and day in all circumstances.

According to Article 18(2), central counterparties shall use scenario-based risk analysis which is designed to identify how various scenarios affect the risks to their critical business functions.

Article 19(1) states that central counterparties shall have in place arrangements to ensure continuity of their critical functions based on disaster scenarios. These arrangements shall at least address the availability of adequate human resources, the maximum downtime of critical functions and fail over and recovery to a secondary site.