12/12/2016

D E C I S I O N

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

FI Ref. 15-9257
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 Stockholm Aktiebolag (556420-8394) a remark.

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

2. Nasdaq Stockholm Aktiebolag shall pay an administrative fine of SEK 30,000,000.

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

To appeal the decision, see *Appendix 1*.

Summary

Nasdaq Stockholm Aktiebolag (Nasdaq Stockholm or the company) is a stock exchange, i.e. a company that holds authorisation to operate a regulated market in accordance with the Securities Market Act (2007:528).

Finansinspektionen has investigated how well Nasdaq Stockholm has complied with certain fundamental requirements that are placed on a stock exchange in accordance with the regulations set out in the Securities Market Act.

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 Stockholm has not had the independent competence or acquired the information required to be able to assess the quality of the delivered services and place sufficient requirements on the supplier. The investigation also shows that Nasdaq Stockholm 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 contingency plan were prepared without consideration for a scenario that manages the risk of cyber attacks.

Because regulated markets play a significant role in the financial system, the requirements on internal governance and control, risk management and information security for a stock exchange are very strict. Finansinspektionen's investigation shows that Nasdaq Stockholm 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 Stockholm. However, the company's infringements have not been so serious that it is necessary to withdraw the company's authorisation. Finansinspektionen is therefore issuing the company a remark and an administrative fine of SEK 30 million.

1 Background

1.1 Operations of the company

Nasdaq Stockholm Aktiebolag (Nasdaq Stockholm or the company) is a stock exchange, i.e. a company that holds authorisation to operate a regulated market in accordance with the Securities Market Act (2007:528). The company is subject to Finansinspektionen's supervision pursuant to Chapter 23, section 1, first and second paragraphs of the same act. Nasdaq Stockholm reported in 2015 annual net sales of approximately SEK 1.46 billion and around 150 employees.

Nasdaq Stockholm 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 Group has a company in Sweden, Nasdaq Clearing Aktiebolag, that holds authorisation to conduct clearing of derivatives as a central counterparty in accordance with 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.

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

1.2 The matter

As part of its supervision, Finansinspektionen initiated a collaboration in June 2015 with the supervisory authorities in Denmark, Iceland and Finland to investigate several of the Nordic subsidiaries of the Nasdaq Group, of which one was Nasdaq Stockholm. Finansinspektionen also conducted an equivalent investigation at the sister company, Nasdaq Clearing Aktiebolag.

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 called "cyber security" in this memorandum. 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 the object of an attack 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 supervision activities was to investigate 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 Stockholm. 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 Stockholm was given the opportunity to respond to Finansinspektionen's preliminary assessment that the company had disregarded its obligations. On 6 July 2016 Nasdaq Stockholm submitted a response to Finansinspektionen. On 26 August, Nasdaq Stockholm visited Finansinspektionen and submitted information verbally.

2 Applicable provisions

Regulated markets play a significant role in the financial system and the requirements placed on a stock exchange are therefore high. The regulations in the Securities Market Act governing stock exchange operations originated from the now repealed Exchange and Clearing Operations Act (1992:543) and Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (MIFID).

The stock exchange's operations are also covered by Finansinspektionen's general guidelines (FFFS 2005:1) regarding governance and control of

financial undertakings, hereafter FFFS 2005:1. General guidelines are not legally binding, but provide guidance in how the requirements of the law may be fulfilled with regard to governance and control. The general guidelines state that the general guidelines are formulated in general terms and allow for alternative solutions, and that it should be possible to explain such solutions. If a company does not follow the general guidelines, it must show how it uses a different approach to fulfil the requirements in the underlying provisions.

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 well Nasdaq Stockholm complies with certain provisions that govern the operations of a stock exchange. 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

One of the fundamental requirements on a stock exchange is that it must conduct its business professionally. It shall also conduct its business in such a manner as to maintain public confidence in the securities market. These requirements are set out in Chapter 13, section 1, first paragraph of the Securities Market Act. According to the third paragraph, point 1 of the same section, a stock exchange shall identify and manage such risks as can arise in its business. The provision was given its current wording with the introduction of the Securities Market Act, but the preparatory work for the law states that corresponding requirements can be said to have been set out already by Chapter 2, section 1 of the Exchange and Clearing Operations Act, which stated, for example, that a stock exchange should conduct its operations as to maintain the confidence of the public in the securities market and in general so that the business could be considered to be sound. [1]

In order to be able to fulfil these requirements, the company should have sound internal governance and control. Finansinspektionen has described in more detail how a company in different respects can achieve sound internal governance and control in FFFS 2005:1. Chapter 7, section 1 of FFFS 2005:1 states that a company may outsource parts of the operations to an external service provider. However, the board of directors and managing director shall at all times be responsible for the outsourced activities. In order to fulfil this requirement on responsibility, it is important that the board of directors and managing director ensure that the outsourcing occurs in a manner that guarantees sufficient governance and control of the function.

According to Chapter 7, section 2 of FFFS 2005:1, the board of directors or the managing director should draw up internal rules for the outsourcing of

[1] Bill 2006/07:115, pp. 383 and 608.

operational functions. These rules should state the demands imposed on the company's order placement expertise, the manner in which risks associated with outsourcing are to be managed and the manner in which the company shall govern and monitor performance of the engagement and review the outsourced activities. The internal rules should also state that the company shall prepare contingency plans and strategies for how the engagement might be discontinued and the activities resumed by the company, and that a written agreement shall be prepared which regulates the service level. According to Chapter 4, section 2 of FFFS 2005:1, the board of directors should ensure that the company's risk management and risk control are satisfactory.

As previously mentioned, Nasdaq Stockholm 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. In accordance with FFFS 2005:1, the company has prepared internal rules – a policy – for the outsourcing of operational functions.

At the time of the investigation, there was a general main agreement between the parties for all services that Nasdaq Stockholm 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 (SLAs). There were appendices to the main agreement that contained brief descriptions of the services, but no detailed quality measures, even though the company's policy for outsourcing states that the precise requirements must be specified in an SLA.[2]

Nasdaq Stockholm 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 delivery, even though the company's policy for outsourcing prescribes that outsourced functions must be evaluated on an ongoing basis in accordance with the monitoring process that is described in each outsourcing contract.[3]

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

Nasdaq Stockholm's outsourcing policy contains provisions that the contract must include conditions ensuring that the contract can be discontinued. However, the policy does not contain provisions requiring the preparation of contingency plans and strategies for how the engagement can be discontinued and the activities resumed by the company without significant disruption in

[2] "...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."
[3] "Each individual arrangement where material activities have been outsourced must be assessed on an ongoing basis according to the monitoring process described in each outsourcing contract."

important activities. The main agreement does contain conditions for discontinuation, but at the time of the investigation there was no in-house expertise for resuming the activities at the company or a strategy or plan for how such a resumption of services would be carried out. Neither was there any information about other suppliers that could be a realistic alternative to the current solution, if resuming the services at the company would not be an option.

In its response, Nasdaq Stockholm 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. Nasdaq Stockholm furthermore states that the company's CEO is responsible for all outsourcing and that the CEO draws on the company's Enterprise Risk Manager (ERM), a person who works with risk management in the company, in risk evaluation and follow-up of the service delivery. According to the company, there is therefore sufficient expertise for evaluating the provided services and efficiently monitoring the outsourced functions. According to the response, ERM reports to the head of the Group's Global Market Operations Department. Nasdaq Stockholm also emphasises that the Board of Directors has taken responsibility for the company's outsourced services, in part by preparing an outsourcing policy.

In its statement, Nasdaq Stockholm also explains 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 functions. Furthermore, the company's management team and Board of Directors have received follow-up reports through the annual overview of, for example, the main agreement. The company also takes the position 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.

With regard to Nasdaq Stockholm's preparedness to resume the services, the company states that a separate plan would have a limited effect, in part because the matter refers to an outsourcing within the Group and in part because of the nature of the services in question. The company states, however, that a separate plan will be prepared.

Finansinspektionen notes that Nasdaq Stockholm takes the position that regular reports have been submitted and to demonstrate this attached an overview of the reporting procedures submitted by the ERM. However, there are no minutes or other documents 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 other type of document that shows that the company has conducted documented follow-up of the supplied

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.

With regard to the expertise that is required to govern and monitor how the engagement has been carried out and review the outsourced activities, Finansinspektionen has noted the following. Nasdaq Stockholm states that the company's CEO draws on the ERM in the work with risk evaluation and follow-up of the service delivery, and that the company thus considers that it has sufficient expertise to evaluate the services and efficiently monitor the outsourced functions. It is also clear that the ERM – even if he does provide support to the company's CEO – primarily reports to the head of the Global Market Operations Department, i.e. a representative for the service provider. Finansinspektionen thus takes the position that the company does not have the independent order placement expertise that is needed to evaluate the provided services and monitor the outsourced functions.

Due to the deficiencies that have been described above, Finansinspektionen makes the assessment that Nasdaq Stockholm has not evaluated the provided services on a regular basis in accordance with the company's policy for outsourcing. It has also not been possible for the company to govern, monitor and review the outsourced functions. The policy does not contain rules requiring the preparation of contingency plans and strategies for how the engagement may be discontinued and the activities resumed by the company. Such plans and strategies have not existed either. Finansinspektionen therefore makes the assessment that the company in this respect has not followed the general guidelines in Chapter 7, section 2 of FFFS 2005:1 when preparing the company's outsourcing policy and that the company has not followed the policy itself, either.

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 and following up on the risks that arose from the outsourcing of the company's information security. Finansinspektionen therefore makes the assessment that the company has not had satisfactory risk management and risk control in conjunction with the outsourcing and that the company has thus not complied with Chapter 4, section 2 of FFFS 2005:1.

In Finansinspektionen's opinion, the above-mentioned deficiencies show that the company to a large extent has relied on the service provider's expertise and competence. Finansinspektionen makes the assessment that the Board of Directors, with regard to cyber security, has delegated in practice its

responsibility to the service provider and that the outsourcing thus has not occurred in compliance with Chapter 7, section 1 of FFFS 2005:1.

In summary, Finansinspektionen notes that Nasdaq Stockholm complied with neither the general guidelines regarding outsourcing of operations in Chapter 7, sections 1 and 2 of FFFS 2005:1 nor the general guidelines regarding internal rules for management and control of risks in Chapter 2 of FFFS 2005:1 in conjunction with the outsourcing of its information security. The company has also not shown that the outsourcing of its information security function in any other way has fulfilled the fundamental requirements set out in Chapter 13, section 1, first paragraph of the Securities Market Act, that a stock exchange shall conduct its business professionally and in such a manner as to maintain public confidence in the securities market. Neither can the company be considered to have identified and managed the risks that may arise in its business in accordance with Chapter 13, section 1, third paragraph, point 1 of the Securities Market Act.

3.2 Risk management

One of the fundamental requirements that is placed on a stock exchange is that it shall identify and manage the risks that may arise in its business. This is set out in Chapter 13, section 1, third paragraph, point 1 of the Securities Market Act, which is supplemented by Chapter 4 of FFFS 2005:1 regarding the management and control of risks. Chapter 4, section 2 of FFFS 2005:1 states that the board of directors should ensure that the company's management of risks (risk management) and follow-up of the company's risks (risk control) are satisfactory. For this purpose, the company should adopt internal rules regarding risk management and risk control. The company should ensure compliance with these rules on a regular basis. According to section 3 of the same chapter, there should be a composite function for independent risk control at the company. The function should provide the board of directors and the management team with information that offers a comprehensive and factual representation of the company's risks and contains risk assessment analyses.

3.2.1 Deficiencies in risk management

As described earlier in this document, large parts of the company's business are outsourced within the Group. Decisions regarding cyber security are largely made by the parent company, which is also the service provider, using informational considerations made by global risk management bodies. Given this background, it is important to consider a local risk perspective and ensure that the global body is provided with information that is relevant from both a local perspective and the perspective of the company. The information that the company submitted regarding 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 Stockholm 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 Stockholm did not ensure that the company's local risk perspective was taken into account with regard to cyber security. Neither has Nasdaq Stockholm 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 Nasdaq Stockholm has not had adequate risk management and risk control with regard to cyber risks. The risk information that Nasdaq Stockholm has had access to has not provided a sufficiently comprehensive and factual overview of all of the company's risks. The company has thus not followed the general guidelines regarding internal rules for management and control of risks and how the risk control function shall be organised as set out in Chapter 4, sections 2 and 3 of FFFS 2005:1. Nasdaq Stockholm has also not shown that it any other way has fulfilled the requirement set out in Chapter 13, section 1, third paragraph, point 1 of the Securities Market Act that a stock exchange shall identify and manage the risks that may arise within its business.

3.2.2 Deficiencies in the Board of Director's determination of risk appetite or risk tolerance for cyber risks

The investigation shows that Nasdaq Stockholm's Board of Directors has not made independent decisions regarding the risk appetite or risk tolerance 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 Stockholm 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 Stockholm at the time of the investigation made any independent decisions regarding risk appetite or risk tolerance.

Finansinspektionen also noted that Nasdaq Stockholm has not had a process for linking its risk appetite or risk tolerance to its financial considerations.

Nasdaq Stockholm explains 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 Nasdaq Stockholm at the time of the investigation had not decided on its risk appetite or risk tolerance with regard to cyber risks. In Finansinspektionen's opinion, this means that the company has not identified, managed or followed up on cyber risks in a satisfactory manner. The Board has also not had a sufficient basis on which to be able to assess and make decisions about risk management and risk control. Finansinspektionen also believes that the Board and the management team have not ensured that the company's internal rules state how the company should manage and control cyber risks. The company has thus not followed the general guidelines set out in Chapter 4, section 2 of FFFS 2005:1 regarding internal rules for management and control of risks.

An important part of risk control is determining the economic consequences that will result from various positions with regard to risk tolerance or risk appetite. The investigation shows that the company has not had a process for linking decisions about its risk appetite or risk tolerance to financial considerations. As a result, there have not been any clear rules for how a change in the threat profile affects which investments in cyber security are needed. The Group's risk management strategies have thus not been anchored in the company's financial plans, which could result in Nasdaq Stockholm not having financial contingencies for managing the risks. Finansinspektionen makes the assessment that the lack of internal rules with regard to risks and financial preparedness means that the company's management and control of cyber risks have not been satisfactory. The company has thus not followed the general guidelines set out in Chapter 4, section 2 of FFFS 2005:1 regarding internal rules for management and control of risks.

In summary, Finansinspektionen notes that Nasdaq Stockholm has not followed the general guidelines set out in Chapter 4, section 2 of FFFS 2005:1 regarding internal rules for management and control of risks. The company has also not shown that it any other way has fulfilled the requirement set out in Chapter 13, section 1, third paragraph, point 1 of the Securities Market Act that a stock exchange shall identify and manage the risks that may arise within its business.

3.2.3 Deficiencies in risk management in collaborations that require technological contacts

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

Finansinspektionen makes the assessment that the lack of insight into the cyber security of the parties with which Nasdaq Stockholm has technological contact could lead to the risks associated with these technological contacts not being considered or 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 Stockholm 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 Stockholm and other parties with which the company has technological contact, Finansinspektionen makes the assessment that Nasdaq Stockholm in this respect has not had a comprehensive and factual view of the company's risks and that the company thereby has not followed the general guidelines set out in Chapter 4, section 3 of FFFS 2005:1 regarding the organisation of the risk control function. The company has also not shown that it any other way has fulfilled the requirement set out in Chapter 13, section 1, third paragraph, point 1 of the Securities Market Act that a stock exchange shall identify and manage the risks that may arise within its operations.

3.3 Business continuity

According to Chapter 13, section 1, third paragraph of the Securities Market Act, a stock exchange shall identify and manage the risks that may arise in its business and have secure technical systems. Chapter 3, section 4 of FFFS 2005:1 states that a company can achieve sound internal control in part by "ensuring continuity in the operations and protecting the assets of the undertaking and the customers, through information security and physical security controls". Chapter 7, section 2 of FFFS 2005:1 also states, with regard to outsourcing agreements, that the internal rules regarding the outsourcing of operations should state that the company and the service provider shall prepare

and maintain contingency plans for unforeseen events, including crisis and catastrophe planning, which shall be tested regularly.

In order to achieve business continuity, Nasdaq Stockholm has prepared continuity plans. According to the information from the company, however, 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 the company would be able to resume critical functions or IT systems in a timely manner.

Nasdaq Stockholm 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 Stockholm 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 these 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.

Since scenarios related to cyber attacks have not been included in Nasdaq Stockholm's risk analysis, the company has not had a sufficient analysis and planned measures for being able to maintain its data authenticity or protect its data integrity in situations where the information has been manipulated or corrupted. There has thus been a risk that Nasdaq Stockholm would not have sufficiently preparedness to be able to resume critical functions in a timely manner.

Because there was no preparation for cyber attacks or deficient data integrity in the company's contingency planning, Finansinspektionen makes the assessment that Nasdaq Stockholm has not protected the company's or its customers' assets and ensured continuity in the operations through information security and physical security controls.

In summary, Finansinspektionen finds that Nasdaq Stockholm has not followed the general guidelines in Chapter 3, section 4 and Chapter 7, section 2 of FFFS 2005:1. The company has also not shown that it any other way has fulfilled the requirements set out in Chapter 13, section 1, third paragraph of the Securities Market Act to identify and manage the risks that may arise within its business and have secure technical systems.

4 Consideration of intervention

4.1 Applicable provisions

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, Finansinspektionen shall consider previous infringement by the company. During this assessment, Finansinspektionen shall attach special weight to whether the infringements are similar in nature and the time that has elapsed between the various infringements. According to the second paragraph of the same section, mitigating circumstances shall 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 organisation 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.

When determining the size of the administrative fine, 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 Stockholm states in part the following with regard to a possible intervention by Finansinspektionen.

Nasdaq Stockholm believes that the deficiencies that Finansinspektionen highlights in its investigation, when placed against a background of Nasdaq Stockholm'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 Stockholm also states that the company has consistently implemented improvements to rectify deficiencies. Since Finansinspektionen opened its investigation, Nasdaq Stockholm 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 Stockholm 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 Stockholm 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 Stockholm 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 Stockholm 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 Stockholm points out that the deficiencies have not caused any damage to the company's systems or operations or any other parties, and neither introduced risks for the financial system.

4.3 Assessment of the infringements and choice of intervention

Finansinspektionen's investigation shows that Nasdaq Stockholm has not followed all parts of the general guidelines in FFFS 2005:1. The company has also not shown that it in any other way has fulfilled the general requirements set out in Chapter 13, section 1 of the Securities Market Act.

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 the operations. Governance, control and responsibility have to a large extent in practice been transferred to the company's parent company, Nasdaq, Inc. With regard to Nasdaq Stockholm, 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 Stockholm'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 Stockholm 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 Stockholm 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 Stockholm'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 ascertain the extent to which the company has realised profits or avoided costs as a result of the infringements. The fine that Nasdaq Stockholm shall pay will therefore be set at no more than ten per cent of the company's net sales from the immediately preceding financial year according to Chapter 25, section 9 of the Securities Market Act. Nasdaq Stockholm's net sales for the immediately preceding financial year amounted to approximately SEK 1.46 billion. Finansinspektionen may therefore decide on an administrative fine that may be at the most SEK 146 million.

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[4] 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 what amount this administrative 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

[4] 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.

potential effects on the financial system and confidence for the financial market to have been considerable.

When determining the administrative fine, Finansinpektionen, 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 Stockholm 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.

In its statement Nasdaq Stockholm 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 to a significant extent 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 therefore cannot be considered a mitigating circumstance.

After a comprehensive assessment of the circumstances that Finansinspektionen shall take into consideration when setting the administrative fine, Finansinspektionen determines that Nasdaq Stockholm shall pay an administrative fine of SEK 30 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 Stockholm Aktiebolag's CEO

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

FI Ref. 15-9257
Notification no. 1

Remark and sanction fee

Document

Decision regarding a remark and administrative fine for Nasdaq Stockholm 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

Securities Market Act (2007:528)

According to Chapter 13, section 1 of the Securities Market Act, a stock exchange shall conduct its business honestly, fairly and professionally and in such a manner as to maintain public confidence in the securities market.

A stock exchange conducting a regulated market shall apply the principles of

1. free access, whereby each and every party who satisfies the requirements of this Act and the stock exchange may participate in the trading,
2. neutrality, whereby the stock exchange's rules for the trading facility shall apply in a uniform manner vis-à-vis all who participate in the trading, and
3. effective transparency, whereby that the participants receive prompt, contemporaneous, and correct information regarding the trading and that the public has the opportunity to obtain such information.

A stock exchange shall also

1. identify and manage such risks as can arise in the business,
2. have secure technical systems, and
3. identify and manage the conflicts of interest which can arise between the securities exchange or its owner's interests and the interest in operating a regulated market in accordance with the first andsecond paragraphs.

In its rules, a stock exchange may not place unreasonable demands on issuers and participants on a regulated market. The question of what constitutes an unreasonable demand shall be assessed taking into consideration its purpose, EC law and other circumstances.

Finansinspektionen's general guidelines (FFFS 2005:1) regarding governance and control of financial institutions (FFFS 2005:1)

Chapter 1, section 3 of FFFS 2005:1 states that the general guidelines are formulated in general terms and allow for alternative solutions. It should be possible to explain such solutions.

Internal governance and control

Chapter 3, section 4 states that a company may achieve sound internal control by, for example:

- regularly following up on the operations and ensuring that controls are in place which guarantee that reporting appropriately reflects the operations;

- regularly monitoring that resources are used efficiently and in order to achieve the undertaking's goals;
- producing internal regulations, as well as documenting and updating them regularly;
- allocating responsibility and work in such a manner that the risk of conflicts of interest is avoided;
- ensuring that an employee does not handle a transaction alone throughout the entire processing chain (segregation of duties);
- ensuring, through controls, that information is provided in the event developments within a business area deviate from the undertaking's guidelines and targets;
- ensuring, through controls, that the reporting is complete and accurate, transactions are reported on time and that reported transactions are actually implemented;
- ensuring continuity in the operations and protecting the assets of the undertaking and the customers, through information security and physical security controls;
- ensuring that information and reporting systems guarantee current and relevant information regarding the institution's operations and risk exposure, etc.

Management and control of risks

Chapter 4, section 2 states that the board of directors should ensure that the company's management of risks (risk management) and follow-up of the undertaking's risks (risk control) are satisfactory.

Chapter 4, section 3 further states that the undertaking should contain a composite function for independent risk control. The function should inform the board of directors, management and other persons who require the information.

The information should provide a comprehensive and factual representation of the firm's risks and contain risk development analyses. The function should also propose the changes in governance documents and processes which result from the observations regarding risk management.

The function should be answerable to the managing director. It may also be situated so that it is answerable to another senior officer who possesses sound knowledge of the undertaking's risks and is directly subordinate to the managing director. Such person shall not, however, be responsible for the day-to-day business operations.

The function should possess sufficient resources for its duties. The duties should not be carried out by employees who are engaged in the day-to-day business operations.

Appendix 2

Outsourcing

Chapter 7, section 1 states that an undertaking may outsource parts of the operations to an external service provider, whether within or outside the undertaking's own group or group of undertakings. The board of directors and managing director shall, however, at all times be responsible for the outsourced activities.

According to Section 2, the board of directors or managing director should draw up internal regulations as to which licensed operations, or operations that have a natural connection with financial operations or their support functions, may be outsourced and the manner in which such shall take place.

The internal regulation should state at least the following:

- the demands which are imposed regarding the undertaking's order placement expertise;
- the manner in which risks associated with outsourcing are to be managed;
- that the undertaking shall ensure that the service provider protects confidential information with respect both to the undertaking and its customers;
- the manner in which the company shall govern and monitor performance of the engagement and review the outsourced activities;
- the demands which must be imposed regarding expertise of the service provider and internal controls and quality, as well as the service provider's possibilities to perform the engagement in the long term;
- that the undertaking and service provider shall prepare and maintain contingency plans for unforeseen events, including crisis and catastrophe planning, which shall be tested regularly;
- that it must be ensured that Finansinspektionen is able, in the future, to exercise effective supervision over the undertaking as well as that the undertaking's obligations towards Finansinspektionen or the undertaking's customers are not breached;
- that contingency plans and strategies shall be prepared regarding the manner in which the engagement might be discontinued and the activities resumed by the undertaking without significant disruption in important activities;
- that a written agreement shall be prepared which regulates the service level, the parties' rights and obligations, as well as other issues pursuant to these general guidelines.