APPENDIX 3: FINANSTILSYNET'S MONITORING ACTIVITIES

Finanstilsynet's supervision of ICT and payment services – key areas

Supervisory activities are risk-based, and Finanstilsynet gives priority to institutions that have the greatest influence on financial stability and well-functioning markets. ICT risk is assessed, and the institutions' own annual assessments of ICT risk are reviewed. Emphasis is placed on monitoring the organisation of ICT/cyber security work, the security of institutions' ICT systems and the organisation of surveillance activities. The supervision covers overall governance of ICT activities, the institutions' emergency response work in connection with business continuity and disaster recovery systems and the testing thereof, control and monitoring of outsourced ICT operations, the institutions' system access control, the institutions' payment services and ICT systems for detecting money laundering and the financing of terrorism. The use of new technology, major changes in the ICT area and extensive changes in the financial infrastructure are also relevant areas subject to monitoring.

Work on payment systems

The EU's revised Payment Services Directive (PSD2)[1] has been incorporated into Norwegian legislation and will form the basis for the supervision of institutions' payment services. Institutions will be monitored with respect to their compliance with the new regulations relating to payment service systems[2], risk related to payment services and compliance with the duty to report new or changes to existing payment services. Account servicing payment service providers' interfaces (APIs) for trusted third parties' account access will also be followed up, cf. opinion from the European Banking Authority (EBA)[3]. When processing concessions, care will be taken to ensure that the institutions have well-documented procedures in areas relating to ICT and payment services. In addition, Finanstilsynet will monitor whether the institutions have robust payment solutions and have established satisfactory emergency plans for the solutions and the electronic payment system. The cooperation with Norges Bank on the payment system and financial infrastructure will continue.

Follow-up of incidents

Following up ICT incidents is a prioritised part of supervisory activities. Finanstilsynet will continue to closely monitor developments in 2023. When incidents occur, emphasis will be placed on whether the institution identifies causes and takes steps to prevent recurrence. Incidents involving serious irregularities will be monitored throughout the duration of the incident. Countermeasures will be considered. Vulnerabilities identified in the institutions' ICT solutions will also be followed up. Finanstilsynet will continue to make an annual review of incident reporting of the largest institutions. It will also be followed up that both account servicing payment service providers and third-party providers report instances of non-conformance in accordance with PSD2 and that the account servicing payment service providers correct the discrepancies and inform the third-party providers.

Outsourcing of ICT activities

Finanstilsynet will continue to monitor institutions' outsourcing of ICT activities and ensure that the institutions, when entering into a new or amended agreements on outsourcing of ICT activities that are critical or important to the institution, reports this to Finanstilsynet, as required by Section 4c of the Financial Supervision Act, cf. the Regulations on the Obligation to Notify Outsourcing of Activities[4]. Supervisory activity includes monitoring that the institutions prepare risk analyses and make a prudent

[1] Lovdata: [1]On payment services in the internal market (PSD2)
[2] Lovdata: Regulations on Payment Services Systems
[3] EBA's statement on trusted third parties' account access: EBA calls on national authorities to take supervisory actions for the removal of obstacles to account access under the Payment Services Directive
[4] Lovdata: Regulations on the Obligation to Notify Outsourcing of Activities (in Norwegian only)

assessment of the outsourcing relationship, that the agreements are in line with regulations and that the outsourcing is handled in a proper manner by the institution, cf. section 2 of the ICT Regulations.

Emergency preparedness

The work of the Financial Infrastructure Crisis Preparedness Committee (BFI) will continue. BFI reviews incident scenarios and determines whether the responsibilities associated with crisis situations are sufficiently clear. Emergency response exercises are planned for 2023 as well, and countermeasures linked to findings from previous exercises will be followed up.

Special incidents, such as the Covid-19 pandemic, the war in Ukraine and the institutions' organisation of their ICT activities, will be monitored, particularly at key operators in the financial infrastructure.

Finanstilsynet participates in relevant emergency preparedness work initiated by other sectors and in cooperation within the national regulatory framework for managing ICT security incidents, partly through the National Cyber Security Centre (NCSC), established by the Norwegian National Security Authority (NSM).

Finanstilsynet will align its emergency prepardness work and handling of ICT security incidents with NSM's framework for handling ICT security incidents[5]. Finanstilsynet is the sectoral response environment (SRE) in the financial market area and exercises its role in collaboration with Nordic Financial CERT according to agreed information exchange rules. The NSM framework forms the basis for the interaction between Finanstilsynet and Nordic Financial CERT.

Monitoring of the cybercrime threat picture

Finanstilsynet will remain constantly informed of institutions' use of ICT and developments in payment services, including specific developments relating to:

• the cyberthreat picture

• emergency preparedness work targeting digital vulnerability and security

• institutions' organisation and follow-up of security work

• changes in payment services due to the use of new technology (fintech)

• cross-border activities

In 2021, Finanstilsynet and Norges Banks estabished a framework for cybersecurity testing in the financial sector (TIBER-NO), thus aiming to promote financial stability by increasing the resilience of critical functions in the Norwegian financial sector against cyberattacks. The project is followed up by a steering group chaired by Norges Bank with participants from Finanstilsynet. Finanstilsynet will hold regular meetings with institutions and Nordic Financial CERT and participate in the Norwegian Cyber Security Centre (NCSC), the European supervisory authorities' work on ICT security and the European Systemic Cyber Group (ESCG) under the European Systemic Risk Board (ESRB).

Consumer protection

Finanstilsynet will control that institutions establish digital solutions in compliance with the regulations, and that the solutions launched have built-in security and functionality in line with consumer expectations. Emphasis will also be placed on whether the institutions ensure that use of their solutions and services is secure for customers.

In addition, Finanstilsynet will monitor that institutions do not share customer data without consent, and that data do not fall into the hands of unauthorised third parties. Finanstilsynet will also control that the institutions communicate with their customers in a safe and proper manner, which includes not sending or

[5]The Norwegian National Security Authority (NSM): Rammeverk for håndtering av IKT-hendelser (in Norwegian only)

requesting information about the customer or the customer's exposures by email or making customers feel unsure by attaching links in emails or SMS communication.

Payment service systems will be controlled to ensure that they do not require users to accept additional functionality in order to be able to use the service, and that users are given the opportunity to protect themselves against adverse incidents, such as the ability to block their cards against online use.

Based on requirements for reporting fraud relating to the use of payment services, cf. section 2 of the Regulations on Payment Services Systems, Finanstilsynet will examine the total extent of fraud and, when needed, also individual operators.

If incidents occur, Finanstilsynet will follow up that the institutions provide customers with information on how they become affected and how the institution or customers themselves can mitigate the situation.

Finanstilsynet will continue to follow up that banks discharge their responsibilities with respect to compliance with the provisions of the Financial Institutions Act[6] regarding cash services. Finanstilsynet will also control that banks have established solutions in line with the provisions of the Financial Institutions Regulations regarding solutions to meet increased demand for cash in a crisis situation[7].

[6] Lovdata: Act on Financial Institutions and Financial Groups (Financial Institutions Act)
[7] Lovdata: Regulations on Financial Institutions and Financial Groups (Financial Institutions Regulations)