

1. Disclosure of information on measure imposed on credit institution

Information on person responsible for breach	
Business name and registered office of legal person	Addiko Bank d. d., Dunajska cesta 117, Ljubljana, Slovenia
Information on breach	
Description of circumstances and conduct entailing a breach of the Payment Services, Electronic Money Issuance Services and Payment Systems Act (Official Gazette of the Republic of Slovenia, Nos. 7/18 and 9/18 [corrigendum]; hereinafter: the ZPlaSSIED)	<p>On the basis of the request for inspection referenced 0.04.5.3-5/2019-5 of 15 November 2019, the supplementary request for inspection referenced 0.04.5.3-7/2019-1 of 21 November 2019, and the authorisation referenced 0.04.5.3-6/2018-26 of 1 July 2019, between 25 and 28 November 2019 Banka Slovenije staff conducted an inspection of Addiko Bank d. d. (hereinafter: the bank) in the area of payment services, with the aim of examining the bank's compliance in the provision of payment services with the requirements of the ZPlaSSIED, the relevant secondary legislation, and legal acts of the EU and European Banking Authority governing the area of payment services.</p> <p>During the inspection of the provision of payment services, breaches were identified in the areas of security measures with regard to strong customer authentication and the provision of access to payment accounts, owing to which Banka Slovenije imposed an order on the rectification of breaches on the bank.</p>
Nature of identified breaches	Breaches in the area of the provision of payment services
Operational part of the decision by which the relevant proceedings are completed	
<p>1. Addiko Bank d. d., of Dunajska cesta 117, Ljubljana, Slovenia, registration number 1319175000 (hereinafter: the bank), has breached the second paragraph of Article 153 of the Payment Services, Electronic Money Issuance Services and Payment Systems Act (Official Gazette of the Republic of Slovenia, Nos. 7/18 and 9/18 [corrigendum]; hereinafter: the ZPlaSSIED) in connection with Article 5 of Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (hereinafter: the RTS) by failing to ensure by 14 September 2019 the use of strong customer authentication in the initiation of electronic payment transactions within the framework of mobile banking for natural persons where the strong customer authentication contains elements that dynamically link the transaction to a specific amount and a specific payee.</p> <p>To rectify the identified breach, in the initiation of electronic payment transactions within the framework of mobile banking for natural persons the bank must ensure the implementation of security measures with regard to dynamic linking as set out in Article 5 of the RTS.</p> <p>2. The bank has breached the first paragraph of Article 117, the fourth paragraph of Article 118 and the third paragraph of Article 119 of the ZPlaSSIED by failing to provide for, by 14 September 2019, the use of an interface enabling secure communication with payment service providers issuing card-based payment instruments, account information service providers, and payment initiation service providers.</p> <p>To rectify the identified breach, the bank must provide an interface enabling secure</p>	

communication with payment service providers issuing card-based payment instruments, account information service providers, and payment initiation service providers in accordance with the requirements prescribed in Chapter V of the RTS.

3. The bank's management board must submit a detailed action plan stating the measures to rectify the breaches referred to in points 1 to 2 of this order to Banka Slovenije by 28 February 2020. By 28 February 2020 the bank must also report the name of the responsible member of the management board and the names of the responsible persons designated in accordance with the bank's internal organisational structure, or the names of the bank's external contractors, who will be responsible for implementing individual activities to rectify breaches and for preparing and implementing the action plan.

In the action plan, the bank's management board must define the timetable for the implementation of each measure, and the persons responsible for the implementation of each measures or activity in accordance with the bank's internal organisational structure.

4. The bank must rectify the breaches by 1 May 2020, and must deliver a report to Banka Slovenije by 15 May 2020, enclosing documents and other evidence from which it is evident that the breaches have been rectified.
5. In accordance with Article 277 of the ZBan-2, Banka Slovenije shall publish the following information in connection with this supervisory measure after these proceedings have been completed:
 - information on the person responsible for the breach:
 - the business name and registered office of the bank;
 - information on the breach:
 - a description of the circumstances and conduct constituting the breach,
 - the nature of the identified breaches;
 - the operational part of the decision by which the relevant proceedings are completed; and
 - information as to whether judicial review proceedings have been initiated against the decision in accordance with the ZBan-2.

Information as to whether judicial review proceedings have been initiated against the decision in accordance with the ZBan-2

Judicial review proceedings have not been initiated.