PRESS RELEASE

ECB sanctions ABANCA for failing to report cyber incident within deadline

16 December 2022

- ECB-supervised banks must report significant cyber incidents within two hours of detection
- Bank knowingly breached its reporting obligation in February 2019
- ECB imposes €3,145,000 penalty on ABANCA

The European Central Bank (ECB) has imposed an administrative penalty of €3,145,000 on ABANCA Corporación Bancaria, S.A. (ABANCA) after it knowingly failed to report a significant cyber incident to the ECB within the prescribed two-hour deadline outlined in the cyber-incident reporting framework implemented in 2017.

In February 2019 ABANCA became the target of a cyber-attack when its IT systems were infected with malicious software. ABANCA responded by temporarily suspending internet and mobile banking services, ATM services and SWIFT payment services, among other measures.

Despite being aware of its reporting obligation and the significance of the cyber incident as early as 26 February 2019, the bank submitted the required report on the incident 46 hours after the prescribed deadline. The bank's omission hindered the ECB's ability to properly assess ABANCA's prudential situation and to react in a timely manner to potential threats to other banks, what could have had potential consequences on the reputation and the stability of the banking sector as a whole.

The entity promptly addressed the effects of the cyber-incident at the time it occurred. The ECB notes that the penalty relates solely to the breach of a reporting obligation in February 2019 and does not entail any assessment of the soundness of the bank's existing IT systems.

When deciding on the level of a penalty, the ECB applies its guide to the method of setting administrative pecuniary penalties. Out of the severity categories "minor", "moderately severe", "severe", "very severe" and "extremely severe", the ECB classified the breach as severe. More details are available on the supervisory sanctions page.

The bank has the right to challenge the ECB's decision before the Court of Justice of the European Union.

For media queries, please contact Georgina Garriga Sanchez, tel.: +49 152 2255 2184.

Notes

- A cyber incident is a single or a series of unwanted or unexpected "information security events" that have a significant probability of compromising business operations and threatening information security, while an "information security event" is an identified occurrence of a system, service or

network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

- The classification of whether a cyber incident is “significant” is to be carried out by the supervised entity based on specific triggers and thresholds, including the reputational damage, financial impact or triggering of crisis management procedures, among others.
- The ECB’s power to impose sanctions stems from Article 18(7) of Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions.
- The decision imposing a sanction may be challenged before the Court of Justice of the European Union under the conditions and within the time limits provided for in Article 263 of the Treaty on the Functioning of the European Union.

CONTACT
European Central Bank
Directorate General Communications
- Sonnemannstrasse 20
- 60314 Frankfurt am Main, Germany
- +49 69 1344 7455
- media@ecb.europa.eu

Reproduction is permitted provided that the source is acknowledged.

Media contacts

Whistleblowing

Copyright 2023, European Central Bank