Question for written answer E-003305/2019
to the Commission
Rule 138
Marek Belka (S&D)

Subject: Cybersecurity threats to banking systems in the EU

The banking sector relies heavily on IT solutions. Most banking services are provided via the internet and mobile solutions. Criminals may attempt to target customer funds and the personal data of individual clients by taking advantage of inefficient security measures.

Cybersecurity is a top priority for maintaining a high level of confidence in the banking system. However, according to many sources, DG FISMA might not have appropriate resources devoted to this matter. Hence the Commission, while focusing on market regulations, might not sufficiently take into account issues relating to cyber safeguards in the banking sector per se. While DG FISMA has appropriate knowledge about the banking and financial sectors and understands the problems in this field, it has to rely heavily on other Commission services (e.g. DG CONNECT) to oversee the EU's digital single market.

1. Does the Commission plan to change the organisational structure of DG FISMA in order to establish an additional unit or even a special directorate focused strictly on cyber threats?

2. As the methods of committing cyber fraud in the banking and financial sectors develop, what will be the next steps proposed by the Commission to tackle these malpractices effectively?