

Newsletter

Data breach notification obligation has been introduced for players of the financial sector in Russia

December 21, 2018

Dear Ladies and Gentlemen,

We would like to inform you of the data breach notification obligation imposed on certain players of financial sector, **namely payment system operators, money transfer operators and payment infrastructure service providers** within the national payment system of the Russian Federation ("**Institutions**").

The respective amendments to the Regulation of the Bank of Russia No. 382-P "On Information Security Requirements for Funds Transfers and the Bank of Russia's Procedure for Monitoring Compliance with Information Security Requirements Applicable to Funds Transfers" ("**Regulation 382-P**") were introduced on July 1, 2018, and to the Federal Law "On the National Payment System" ("**Law**") on September 29, 2018.

We draw your attention that in the Regulation 382-P the Bank of Russia mentions only money transfer operators and payment infrastructure service providers as those subject to the notification obligation, while the Law also mentions payment system operators as such.

Under the Law all Institutions **are required to notify the Bank of Russia of information security** incidents that caused or might have

caused unauthorized money transfer (without client's consent), and/ or failure to carry out money transfer. In addition, money transfer operators and payment infrastructure service providers **are obliged to notify the Bank of Russia on their plans to make the information about incident publicly available** (e.g., to convene a press conference or issue a press release) as well.

These obligations were clarified in more detailed guidance issued by the Bank of Russia¹ specifying particular timeframes and internal mechanisms to put in place in order to file the said notifications.

From the legal perspective, the issued guidance itself is not legally binding, unless legally binding regulations contain reference to it, or an Institution enters into a so-called cooperation agreement with the Bank of Russia and thereby undertakes to comply with its respective information security standards. However, currently the guidance is the only document clarifying practicalities of the new obligation and the Bank of Russia expects Institutions to follow it. The Bank of Russia will likely stick to the unified approach, so we cannot exclude that the provisions set out by the guidelines will be made legally binding.

We hope that the information provided herein will be useful for you. If any of your colleagues would also like to receive our newsletters, please let us know by sending us his/her email address in response to this message. If you would like to learn more about our **Data**

¹ Standard "Security of Financial (Banking) Operations. Management of Information Security Incidents. On the Form and

Timeframes of Cooperation by the Bank of Russia with the Participants of Information Exchange in case of Detection of Information Security Incidents" (STO BR BFBO-1.5-2018)

Protection and Cybersecurity Practice, please let us know about it in reply to this email. We will be glad to provide you with our materials.

Note: Please be aware that all information provided in this letter was taken from open sources. The author of this letter and ALRUD Law Firm bear no liability for consequences of any decisions made in reliance upon this information.

If you have any questions,
please, do not hesitate
to contact the Partner
of ALRUD Law Firm



**Maria
Ostashenko**

Partner

Commercial,
Intellectual Property,
Data Protection &
Cybersecurity

E: mostashenko@alrud.com

Sincerely,
ALRUD Law Firm