Information Security

Personal data

The Bank complies with both Russian and international laws on personal data processing and protection. The design of current and future processes and products of the Bank assumes obtaining consents from the customers, counterparties, and the Bank's employees for the processing of their personal data, for the minimum use of their data when in interaction between the employees and the Bank's systems, and for the provision of the **«security by design» and «security by default»** concepts. The Bank pays special attention to building relations with counterparties in the process of implementing joint products and services while limiting the use of personal data in the information exchange process as much as possible and protecting personal data during their transfer.

Any improvements in the Bank's systems associated with the processing of customer data and payments should include mandatory testing by the Bank's employees and simulation of hacking to prove the security of upgraded products and systems.

Antifraud actions

The Bank pursues a zero-tolerance policy toward illegal actions against its customers.

For this purpose, the Bank:

- has implemented and maintains fraud monitoring processes for remote banking;
- investigates any attempts of stealing funds from the Bank's customers;
- interacts with the Bank of Russia and other credit institutions, communication service providers, and law enforcement agencies for the exchange of information about the actions of fraudsters and for the timely prevention of fraudulent activities;
- implements the program for enhanced protection of systems and data, which is reviewed annually and updated completely every three years.

The above activities resulted in dozens of prevented attempts of stealing funds from legal entities and individuals, which saved them dozens of million rubles. The only loss by a legal entity because of the fraudster's actions in the remote business education system (RBES) in 2019 amounted to RUB 3,000; the transaction was marked as suspicious but was additionally confirmed by the customer itself.

Cybersecurity (traditional information security)

The Bank pays much attention to information security and resistance to cyber threats.

The following biggest threats for the Bank were identified within the frames of its information security strategy:

- External attacks as a result of actions of hacker groups, which are aimed at stealing data or money via payment systems
- Attacks aimed at customers and stealing customers' funds via remote banking services
- Fraudulent actions of the Bank's employees or counterparties, which may cause data leaks or thefts using authorized access to the information systems of the Bank
- Logical attacks at ATMs (use of special software for money disbursement without using cards and for debiting accounts) and payment terminals (use of special software to reload cards without cash)

The following projects were initiated and successfully finished for the implementation of measures to prevent the materialization of threats:

- Implementation of the **next generation firewall** as a basic element of protection against external attacks
- Implementation of a solution to counter targeted attacks made using malicious emails or malicious websites, which use 0-day vulnerabilities and are not detected by standard means of protection, for example, antivirus software (as a result of system operation, over 650 targeted attacked were repelled)
- Implementation and development of the personnel training system simulating sending of malicious attachments and fishing links by hackers and appointing testing automatically if an employee opens such attachments or types a password to their account on the websites available at the fishing links
- Development and implementation of an antifraud system to identify abnormal and illegal payments sent to the Bank of Russia or to the international data transfer and payment system SWIFT

Identification and elimination of merely technical vulnerabilities typical of information systems and logical vulnerabilities affecting customer service processes and products are the most important processes of information security.

To minimize their probability, the Bank started supporting the following processes in 2019:

- External scanning of vulnerabilities; full coverage was reached for all 179 publications of the Bank's services on the web and external networks, scanning results are recognized by auditors as performed by the Approved Scanning Vendor as part of the PCI DSS standard conformity audits.
- A red team was set up—that is, a group of specialists with qualifications similar to hackers, whose main task is to conduct penetration tests and identify vulnerabilities through the eyes of hackers for the purpose of thorough identification of vulnerabilities that cannot be identified instrumentally.
- Information Security Department participates in, and controls, all tasks of IT development, including the following:
  - Analysis of business requirements
  - Analysis of technical assignments
  - Formation of a set of requirements for the implementation of security-by-design and security-by-default concepts for all services and products developed by the Bank
  - Verification of the fulfillment of requirements before bringing the implemented tasks in action
  - Participation of red team specialists for the purpose of vulnerability analysis in any services published on the web and in any payment applications
- External penetration tests organized by the internal audit are performed by specialized companies with highly proficient specialists.

Therefore, when it comes to the management and elimination of vulnerabilities, in 2019, integral, full-fledged and, most importantly, efficient processes were implemented.

There is a security incidents response team in the Bank to monitor and provide timely response to information security incidents. The work of this team, operating as part of Information Security Department, in 2019 resulted in the creation of the monitoring system architecture, implementation of the subsystem of collection and primary analysis of incidents, implementation of the incident response platform, and automation of the formation of any incidents as tasks for the team members in the implemented platform. The ongoing processes are built so that the time from the attack to the analysis of the processes within the attack and to the termination of the attack usually does not exceed 4 hours.

The quality of information security services has been proven by the audits conducted in 2019 to check conformity to the PCI DSS security standard and SWIFT Customer Security Programme.

MKB pays special attention to raising awareness of market participants about the existing risks, threats, new technologies, and trends in the sphere of information security. The Bank's employees also take part in training seminars, coaching, and various activities dedicated to this issue.

It should be noted that Vyacheslav Kasimov, Director of Information Security Department at MKB, participated repeatedly in various activities and conferences dedicated to the information security as a speaker or an invited expert.

List of events in which MKB took part in 2019

Description of event	Questions discussed
Case forum Fraud in the Financial Sphere. Banks	Contemporary challenges and threats on the part of cyber criminality, methods to identify and prevent fraudulent actions, practical advice on the problems of external and internal fraud
Merlion IT Solutions Summit	The largest annual event of the IT industry where the representatives of the largest Russian and foreign IT companies discussed the most important technological trends, including those related to data flows, principles, and measures of their protection
Vedomosti Conference "Cyber Security: Laws, People, Technologies"	Investments in security, cyber training and stress testing, staff training and selection in the field of information security

"The landscape of criminality changes: it becomes more digital. It naturally entails digitalization of security. Information security comes into the picture in terms of risk mitigation in the organizations. Businesses realize this state of affairs, although they continue to minimize their costs for non-profit-making functions. However, finally, only talented teams who are able to demonstrate a high quality of processes amidst a limited number of resources will be able to achieve success in the field of cybersecurity".

Vyacheslav V. Kasimov
Director of Information Security Department at MKB