UDC: 336.71
JEL: G21

Problems of establishing the practice of remote identification of clients in the Russian banking system (economic aspects)

Y. S. Ezrokh

Novosibirsk State University of Economics and Management,
56, Kamenskaya ul., Novosibirsk, 630099, Russian Federation

For citation: Ezrokh Y. S. (2020) Problems of establishing the practice of remote identification of clients in the Russian banking system (economic aspects). *St Petersburg University Journal of Economic Studies*, vol. 36, iss. 2, pp. 266–286. https://doi.org/10.21638/spbu05.2020.205

The article analyses the economic aspects of establishing the practice of remote client identification by Russian credit institutions. Developing such practices is necessitated by the permanent digitization of the interaction between subjects of banking relations. The article presents the results of an analysis of the economic aspects of remote client identification by banks in developed and developing countries (Austria, Great Britain, India, China, USA, Sweden, Switzerland, and South Korea). The research reveals the theoretical and practical peculiarities of the banking biometric identification system currently functioning in Russia. On the basis of this analysis, the author identifies economic reasons for the lack of motivation of most Russian banks to develop new practices. For the first time in Russian economic literature, the key problems that impede remote client identification have been discussed systematically, including: a) risk of unauthorized access to the central database; b) concerns about privacy violations; c) lack of free access to materials on software testing, guarantees of developer companies, operators, etc.; d) risk of unauthorized access to the UBS by outsiders successfully using identification procedures; e) exposure to financial risks from unauthorized access to the UBS, transferred to clients; f) unsatisfactory results of combating banking cybercrime in Russia. The author advances several robust proposals to overcome these problems and minimize the economic risks of applying remote client identification systems in Russia, taking into account the positive and negative experiences of foreign countries.

Keywords: biometrics, video-identification, UBS, client identification, cybercrime, online identification, fintech, economic risks of remote identification.

Introduction

Global digitization is an inevitable characteristic in the development of the modern economy. On the one hand, it leads to an increase in the commercial efficiency of enterprises, and on the other to an increase in customer satisfaction due to lowered prices for goods and services, better quality of services provided, and so on. At the same time, the transition to remote channels of digital interaction between companies and their clients can entail increased business risks, which negatively affect the motivation and, consequently, the speed of introducing such innovations into many sectors of the economy. For example, banking is one of the most conservative business sectors, and ongoing changes in standardized products (e.g. the possibility to choose your own payment card design)

https://doi.org/10.21638/spbu05.2020.205

are banking marketing activities, i.e. actions that do not change the established system of interaction between credit institutions and their clients. However, in the short term, much may change dramatically in retail banking. On June 30, 2018, the Central Bank of the Russian Federation set about creating a national system of remote client identification by banks (hereinafter the innovative project, the project) following the adoption of Federal Law No. 482-FZ "On introducing amendments to separate acts of the Russian Federation" of December 31, 2017. Meanwhile, domestic banks are obliged to start collecting biometric data of citizens in all their branches by the end of 2019.

This study is comprehensive in nature, which determines the following structure of presentation of information. In the beginning, the fundamental principles of the functioning of the institution of remote customer identification established in Russia were analyzed, on the basis of which the existing economic contradictions were highlighted; this made it possible to formulate a scientific hypothesis, purpose and objectives of the study. Then, on the basis of a literary and practical review, the experience of the functioning of relevant institutions abroad was systematically systematized (by the examples of economically developed and developing countries). The above has become the basis for identifying and formalizing the existing problems of establishing the institution of remote customer identification in the russian banking system (in the economic aspects), as well as justifying strategic measures to overcome them. In the final part, the general foresight risks of global digitalization during the formation of the institute of banking remote biometric identification in Russian are discussed and the results of the study are summarized.

Fundamentals of the functioning of the banking remote identification system in Russia

Remote identification is a mechanism that allows individuals to receive financial services remotely by confirming their identity with biometric personal data (face image and voice) at any bank[1]. Theoretically, a citizen of the Russian Federation can hand over his biometric samples once (free of charge) at one bank and then remotely open accounts, make transfers, apply for loans, etc. in any[2] national credit organizations (Figure 1).

When the client applies to register biometrics, the bank performs the identification in the traditional way (by passport) and enters the client's data into the USIA (if the client has not previously been registered on the public services portal). Then, the client is videotaped and his voice is recorded by repeating all digits three times (in descending and ascending order, as well as in a random sequence). After successful biometric registration, customers can access the services of those banks whose software supports remote bio-identification. This procedure is as follows: on the website of the relevant credit institution the client enters the section "Internet bank"/ "online bank" or downloads the bank's mobile application to a smartphone. The client then passes a simple primary registration and is redirected to

[1] Central Bank of the Russian Federation. URL: http://www.cbr.ru/fintech/remote_authentication/ (accessed: 11.02.2019).

[2] The Central Bank of the Russian Federation compiles a special list on a monthly basis of banks to exclude institutions: a) non-licensed to attract funds of individuals; b) to whom measures to prevent bankruptcy of banks are applied; and c) to whom the Central Bank prohibited remote identification. Additionally, banks can independently deny clients remote identification if: a) the citizen is on a special "black list" (on grounds of terrorism, extremism); the bank has substantiated suspicions (Materials of ConsultantPlus. URL: http://www.consultant.ru/document/cons_doc_LAW_32834/ (accessed: 12.01.2019)).

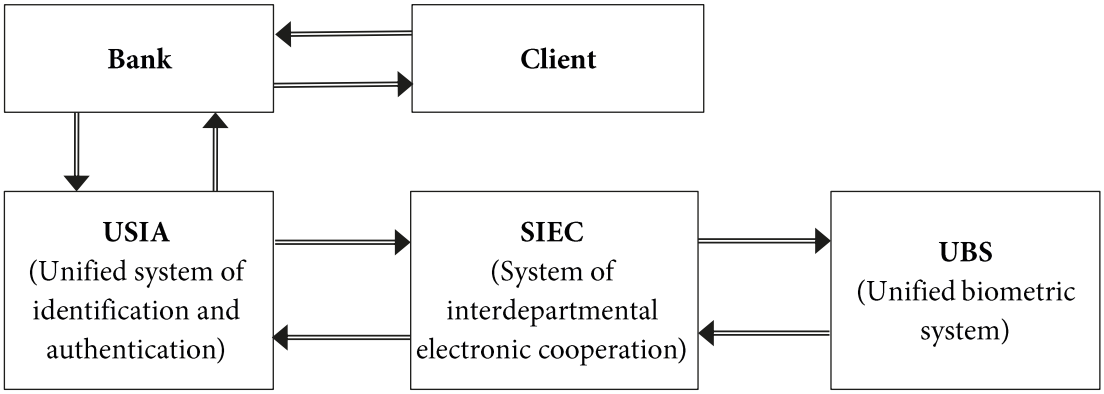

Fig. 1. Simplified scheme of biometric registration process

Note: the dashed line shows the reverse transmission of information; Rostelekom PJSC is the operator of USIA and UBS, the Ministry of Communications and Mass Media of the Russian Federation is the operator of SIEC.

Based on: the methodological recommendations of Rostelecom on working with the Unified Biometric System (version 1.12) (Materials of Rostelecom. URL: https://bio.rt.ru/upload/iblock/a8f/Metodicheskie-rekomendatsii-po-rabote-s-Edinoy-biometricheskoy-sistemoy-_Versiya-1.12-ot-13.09.2018_.pdf (accessed: 12.01.2019)).

the USIA website, where he enters a login and password, and then completes his biometric verification with the help of the UBS[3].

Remote identification systems will soon be universal. In theory, the system will increase the accessibility of banking services for all residents of Russia, as small or remote settlements often have no bank branches at all, or only a Sberbank branch (i.e. there is no competition). In megacities, personal visits to bank offices are inhibited by the shortage of car parking and the ever-increasing pace of life. At the same time, the "transfer" of customer services to the "virtual world" can significantly reduce bank expenses (personnel, premises, office equipment, etc.) and increase the accessibility of financial services.

Economic contradictions, hypothesis, research aims

Despite the economic attractiveness of a remote identification system, less than 3 000 biometric templates were created *throughout the country* in the first four months of its operation[4]. No other official data has been published either by the Central Bank or the business media. In addition, the number of banking offices conducting biometric identification of clients has not increased, but instead has decreased. In 2019, "Russians refuse *en masse* to submit biometrics to banks"[5]. This indicates a serious economic contradiction. On the one hand, on the initiative and with the active participation of the mega-regulator of the financial market (the Central Bank), Russia has established an institution of remote biometric identification of clients by banks, the functioning of which should increase:

[3] The SIEC is not used in remote identification procedures (i.e. later). Instead, biometric identification is carried out through vendors, companies that have signed relevant agreements with Rostelekom. For example, Tinkoff Development Centre is one organization that is "authorised to conduct recognition of customer voice samples in the process of remote identification" (Materials of TASS. URL: https://tass.ru/ekonomika/5695468 (accessed: 12.01.2019)).

[4] Newspaper "Vedomosti". URL: https://www.vedomosti.ru/finance/news/2018/11/12/786133-proverke-tsb-k-sboru-biometrii (accessed: 11.02.2019).

[5] 360.tv. URL: https://360tv.ru/news/tekst/rossijane-otkazalis-sdavat-bankam-biometriju/ (accessed: 07.01.2019).

a) the efficiency of the financial and credit system of the country as a whole, and b) the level of consumer satisfaction. However, in reality, both banks and individuals show low interest in the development of an innovative institution. The former try to comply only with formal requirements of the Central Bank for participation in the process (not to be subject to penalties), and the latter try to avoid providing biometric samples[6].

This allows us to formulate our main hypothesis: there are a number of significant economic problems in developing remote biometric identification of clients in Russia's banking system initiated by the Central Bank, resulting from the lack of economic interest by credit institutions and by citizens in active and voluntary participation. An integrated approach is required to overcome these constraints. Thus, the main goal of this research is to develop a set of measures to overcome current problems connected with the formation of remote client identification in the Russian banking system. To achieve this goal it is necessary: a) to study international experience in the relevant field; b) to conduct a comprehensive analysis of objective reasons for low motivation among Russian banks and their clients to participate in the formation and development of remote biometric identification; c) to formulate and structure key problems; d) to examine problematic areas in state policy and measures of cybercrime prevention in the banking sector of Russia, which impedes the development of remote biometric identification of clients by banks; e) to provide justification for the measures and means for overcoming the identified problems; and f) to identify the general risks of global digitization, which should be taken into account when exercising regulatory influence on the development of remote biometric identification in the medium and long terms.

Literature review

Almost all modern economists agree that digitization has a serious impact on the evolution of "familiar tools for managing banking products and services" [Kozlova, Ustinova, 2019]. According to experts at Digital McKinsey, "in Russia the penetration of remote banking services falls behind the penetration of the Internet, which indicates the potential for its further growth"[7]. At the same time, the ongoing "digital revolution" in modern Russia and in most developed and developing countries makes remote maintenance a key technology that allows a bank to intensify its growth in a saturated market and increase its competitiveness [Vengerovskij, 2018; Martens, 2018].

One essential requirement for remote banking is to carry out procedures for remote identification of the client. As E. V. Chaikina noted, "without remote identification, it is difficult to introduce new financial technologies" [Chajkina, Kozinkin, Chajkin, 2018, p. 114]. At the same time, the procedure, despite the absence of personal contact between client and authorized bank employee, should be legally binding. It is obvious that "any legal solutions technologically depend on the nature and functioning of digital technologies" [Naumov, 2018, p. 126], entailing the risk of loss both on the part of banks and their clients due to malicious actions of third parties. These risks are managed from two sides: by the

[6] Thus, some banks "require their clients to submit biometric data on a mandatory basis" (Banki.ru. URL: https://www.banki.ru/news/bankpress/?id=10898888 (accessed: 19.01.2019)).

[7] Mckinsey's materials. URL: https://www.mckinsey.com/ru/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Russia/Our%20Insights/Digital%20Russia/Digital-Russia-report.ashx (accessed: 25.01.2019).

bank's compliance control services inspecting suspicious transactions [Emets, 2019], and by improving identification procedures. In foreign countries, institutions apply diverse types of biometric identification not because of "their innovative nature, but because they are available and accessible for all citizens, regardless of the level of literacy and education" [Dostov, Shust, Kozyreva, 2017, p. 104].

Unfortunately, in modern Russian science, issues of biometric identification of clients in the banking sector are covered in a fragmented manner, which is largely due to the novelty of the subject. Most authors focus on technical aspects of various types of biometric identification [Lozhnikov, 2017; Yakimenko, Vikhman 2016] and there is very little research on their economic aspects[8]. S. V. Krivoruchko notes that such technologies "increase the indicators of accessibility of payment services in the world and in the Russian market of non-cash transactions" [Krivoruchko, Maklakova, 2017, p. 186]. The work of E. A. Medvedev briefly summarises the applied aspects of the system of remote identification of bank borrowers at Home Credit Bank [Medvedeva, 2018]. At the same time, there are no works devoted to problems of forming remote client identification in the Russian national banking system. It is important to emphasise that the structure of foreign research is generally similar to Russian research, with a general focus on technological [Awad, 2016; Kumar, 2019] rather than economic issues [Indrayani, 2014; Gelb, Decker, 2011] in the operation of identification systems and models in the banking sector. Economists generally agree that "providing simple and secure online access to banking systems through biometrics is a priority for banks" [Charles, 2018, p. 91].

The above makes it particularly important to study the experience of foreign countries in the field of formation, functioning, and future development of remote client identification.

Banks' worldwide practice of remote client identification

These systems have been functioning in a number of foreign countries for quite a while [Krivoruchko, Ponomarenko, Lopatin, 2019][9].

Indian experience. The world's largest repository of biometric templates is the Unique Identification Authority of India (UIDAI). Since 2009 it has accumulated biometric information of more than 1 bln users' fingerprints and irises [Banerjee, 2015]. However, in January 2018 *The Tribune* published results of an investigation, according to which it only costs 8 doll. and takes 10 minutes for an anonymous hacker to provide journalists with access rights to the UIDAI database, plus another 5 doll. to buy a program to fabricate ID-cards of a country's resident". (Although not for a complete passport replacement, this can be used to perform a wide range of banking and other operations)[10]. Further, the

[8] A significant share of research, however, is conducted by students [Krylova, Rudakova, 2018; Nazarov, 2018; Shnekutis, Gobareva, 2018].

[9] Some interesting information can also be found in the report of the Central Bank of the Russian Federation ("Review of the international market of biometric technologies and their use in the financial sector") (Central Bank of the Russian Federation URL: https://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf (accessed: 12.02.2019)). However, it is carried out in a referential and "positive" way, i.e. without critical analysis of "problem areas". Materials in this paragraph are not excerpts from this review; they have been obtained by the author through an independent analysis of a wide array of foreign primary sources.

[10] Materials of the newspaper Tribune-India. URL: https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html (accessed: 02.02.2019).

NGO "Center for Internet and Society Studies" presented a convincing report, according to which confidential information from the UIDAI database appeared publicly on government websites at least *four* times[11].

Swiss experience. In March 2016, the Swiss Financial Market Supervisory Authority (FINMA) for the first time permitted video and online customer identification, the results of which were deemed the equivalent of a personal visit to a bank's office. The idea here is to enable bank employees to communicate with clients "live" through a "teleconference bridge", where the clients answer various questions, and present their passports and other documents (including tilting them to verify whether holograms are present). There is no direct interaction with the client in online identification, which necessitates stricter procedural requirements. First, the bank has to ensure that the person whose identity is being verified will make a transfer from his or her account to an account opened with any Swiss bank or bank in Liechtenstein. Second, the client has to confirm his or her residential address (e.g. utility bills, postal receipts, etc.).

Following the *success* of the online identification system, the regulator (FINMA) lowered requirements in July 2018. Thus, video identification no longer required sending one-time SMS passwords, and online identification made the mandatory transfer requirements simpler (previously, the sender's bank had to be located in Switzerland or Liechtenstein)[12].

Austrian experience. In January 2017, the Austrian Financial Market Authority (FMA) allowed local banks to conduct video identification of clients, with mandatory storage of an electronic file recording all stages of the procedure. High quality screenshots (separate photos) of the client's face, and the front and the back of the identity document were to be produced[13]. For example, a large Austrian bank Erste Bank und Sparkassen conducts video identification of new clients from 8:00 to 12:00 daily, with the process taking no more than ten minutes[14]. The development of innovative technologies in Austria is largely based on (and mirrors) the successful experience of Germany.

Swedish experience. In 2002, a number of major Swedish banks (Handelsbanken, Swedbank, etc.) established the company Finansiell ID-Teknik, whose function was to operate the digital identification platform BankID[15]. Within this platform, clients can remotely receive banking services, submit various documents to government agencies (declarations, applications, etc.), and execute contracts with various companies. The BankID system, however, does not require the client's biometrics analysis, using a traditional login and password for identification[16]. These can be obtained via: a) a personal visit to the bank office; and b) existing Internet banking systems. There is no possibility of remote opening

[11] Materials of Center of Internet & Society. URL: https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof/ (accessed: 03.02.2019).

[12] Instead, there was introduced an automated verification of whether a person undergoing online identification is a living being (Eidgenössische Finanzmarktaufsicht FINMA. URL: https://www.finma.ch/en/news/2018/07/20180717-mm-video-online-id (accessed: 03.02.2019)).

[13] The Financial Markets Authority (FMA). URL: https://www.fma.gv.at/download.php?d=2665 (accessed: 02.02.2019).

[14] Erstegroup. URL: https://www.erstegroup.com/en/news-media/press-releases/2017/01/23/erste-bank-introduces-video-based-identification-of-new-customers-alias (accessed: 07.02.2019).

[15] Bankid. URL: https://www.bankid.com/en/om-oss/about-finansiell-id-teknik (accessed: 07.02.2019).

[16] To increase security, the information on personal BankID can be stored on a plastic smart card. It is inserted into a special card reader (similar to those used in "usual" ATMs and payment terminals), which is then connected to a computer. The card reader is issued by the servicing bank (Bankid. URL: https://support.bankid.com/sv/bestalla-bankid/bestalla-bankid (accessed: 08.02.2019)).

of bank accounts. A client must at least once provide personal identification in one of the banks. The number of unique BankID users is constantly increasing. As of November 1, 2018 it exceeded eight million people. Given that the total number of Swedish residents is tne million, on average the service covers 80 % of the total population, the figure being even higher among people aged 21 to 50 years — 95–97 %[17].

The experience of the UK and US banks. In 2006, the UK adopted the Identity Cards Act, under which the National Identity Register was established. The Register collected personal data of the citizens, including biometric information. Four years later, however, both the Act and the Register ceased [Martin, 2012]. The United States has never had a national biometric databank[18].

Currently, most financial institutions do not use or support primary remote client identification, including the Bank of America[19], Barclays[20], and others. To register online in traditional Internet banking or mobile banking systems, a citizen should already have an active account, a payment card, etc. There is also a crucial difference between authentication when using web-banking (traditional "client-bank" system launched on personal computers) and mobile banking, i.e. applications that work on smartphones. In the first case, "classic" passwords consisting of numbers, letters and (or) signs are used to log in[21]. In the second, the customer's fingerprints or a selfie (online photo) may be used to access the site. Such options are offered by Citi, Royal Bank of Scotland, Wells Fargo, etc.[22]

What is characteristic of the bioidentification systems described is that banks do not collect clients' biometric data in advance or during the maintenance process. Neither do they store, transfer, verify, or protect data. All technical aspects (and liability) rest entirely on smartphones, which send a command to the bank's mobile application.

The experience of South Korea. In April 2018, the government abolished the compulsory identification of banks' customers via "traditional" passports or electronic signatures certified by the unified national government certification system (the latter has been in force for the last 20 years). In just three months, the Korean Federation of Banks (KFB) announced the launch of the private block system BankSign (developed by Samsung)[23]. It allows clients to perform transactions using mobile banking systems of *different* banks, provided they initially have an account (bank account) in *one* of them. Personal identifiers may include fingerprints, "traditional" passwords and other templates[24]. They are verified by smartphones (there is no national repository of personal data), with blockchain technology preventing illegal use of stolen personal data for counterfeiting electronic access

[17] Bankid. URL: https://www.bankid.com/assets/bankid/stats/2018/statistik-2018-10.pdf (accessed: 06.02.2019).

[18] The United States does not have a single "national identity card"; a driver's license is often used as an identification document.

[19] Bank of America. URL: https://secure.bankofamerica.com/login/enroll/entry/olbEnroll.go (accessed: 01.02.2019).

[20] Barclays bank. URL: https://bank.barclays.co.uk/olb/authlogin/loginAppContainer.do /identification (accessed: 02.02.2019).

[21] Wells Fargo bank. URL: https://connect.secure.wellsfargo.com/auth/login/present (accessed: 11.02.2019).

[22] Citi bank. URL: https://online.citi.com/us/jrs/pands/detail.do?id=citimobilesmartphones&jfp_token =spbtlwis (accessed: 11.02.2019).

[23] CCN. URL: https://www.ccn.com/banksign-samsung-blockchain-south-korea/ (accessed: 11.02.2019).

[24] Samsung. URL: https://www.samsungsds.com/global/en/about/news/banksign.html (accessed: 11.02.2019).

certificates. Unlike all the above systems, electronic access is subject to periodic (once in 3 years) prolongation, which can be carried out only after personal identification of the client. Unlike all systems considered above, electronic access is subject to periodic (1 time in 3 years) prolongation, carried out only after personal identification of the client. At the end of 2018, the BankSign system was primarily offered by mobile banking. However, many major Korean banks (KEB Hana, Woori, etc.) are adapting the technology for web-banking systems to be used by enterprises (planned to be completed by the 1st half of 2019)[25].

The Chinese experience. China is currently conducting several simultaneous experiments on remote identification of people that banks could introduce in the short and medium terms [Khan, 2018]. First, since 2015 the Ministry of Public Security has been working on developing a powerful facial recognition system to allow banks to identify any citizen within three seconds (with an accuracy of 90 %)[26]. Second, in Guangzhou Province since 2017, any user of the WeChat national messenger (WhatsApp analogue) can obtain a virtual identification card (analogue of the government passport)[27]. After the recognition of a person with a smartphone, a citizen will be able to access government, banking, and other services.

Conclusions regarding foreign experiences. First, the interest of both clients and banks in remote identification is increasing across the world. This leads to a gradual liberalization of banking rules, especially in developed countries. *Second*, principles and rules of using remote identification of clients by banks in all countries differ significantly, and there is no single approach to remote identification[28]. *Third,* developed countries have not chosen the option to create a single (national) data base of citizens' biometrics. Instead, many European banking systems have been developing a hybrid system of video identification of new clients (e.g. Austria and Switzerland). *Fourth*, the UK and the USA have no primary remote identification at all. At the same time, many large banks allow their clients an opportunity common in many countries (including Russia) to access mobile banking services from smartphones, using fingerprints or selfies. At the same time, new customers can open a bank account only if they personally visit the bank. *Fifth*, in a number of developed countries (e.g. Sweden) traditional (not biometric) methods of remote client authentication — logins, passwords, card readers — continue to be used successfully. *Sixth*, the most "IT advanced" countries have already created more secure block-chain platforms for remote identification, which run on "ordinary" gadgets (i.e. without a national biometric databank). *Seventh*, in a number of countries (e.g. South Korea) customers need to renew their identification periodically (every three years) by personally visiting a bank's branch to continue using remote services. *Eighth*, a number of high-profile hacker attacks on national biometric databanks took place in a number of developing countries (e.g. India) in 2018. As a result, confidential information of a large number of users (e.g. 55 mln people in the Philippines) was disclosed to the public[29]. *Ninth,* many countries (e.g. China) first

[25] Etnews. URL: http://english.etnews.com/20181008200002 (accessed: 12.02.2019).

[26] SCMP. URL: https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any (accessed: 12.02.2019).

[27] SCMP. URL: https://www.scmp.com/tech/social-gadgets/article/2125736/wechat-poised-become-chinas-official-electronic-id-system (accessed: 15.02.2019).

[28] There are many various biometric parametres, including keyboard rhythm [Lozhnikov, 2017].

[29] Association of progressive communications. URL: https://www.apc.org/sites/default/files/Briefing-National-ID-3.pdf (accessed: 15.02.2019).

conduct long-term testing of new systems and pilot operations in small areas: a) to debug processes, and b) to reduce potential commercial and reputational risks when implementing relevant innovations on a full scale.

All of the above determines the particular importance of analyzing the problems of the system of remote client identification emerging in Russia, as it is of a potentially "dangerous" nationwide nature.

Involvement of Russian banks in developing the institute of remote client identification: Challenges

Regardless of the position of the Central Bank of Russia, which supports the rapid development of this innovative project, the overwhelming majority of 410 domestic banks[30] involved *de facto* refused to collect client biometric data (Figure 2).

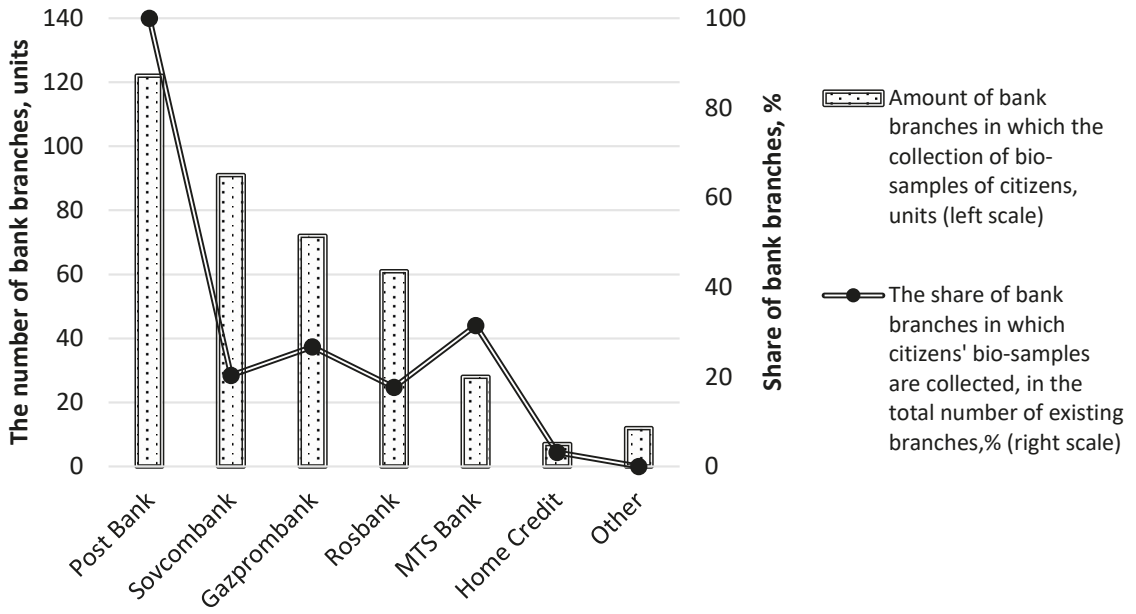

Fig. 2. Information on the number and share of banks collecting the biometric data of citizens (as of December 1, 2018)

Note: the "other" category includes 11 banks, among which there are small regional credit institutions (Ural FB, Kamkombank, etc.) that collect customer biodata only in 1–2 offices.

Based on: Central Bank of the Russian Federation. URL: http://www.cbr.ru/fintech/remote_authentication/map/ (accessed: 15.01.2019).

Only six large and medium-sized banks are actively involved in the widely announced innovation project, with all of them, except the Post Bank, piloting relevant services in a number of selected offices (from 3 to 30 % of the total number). However, by December 1, 2018, the total number of bank branches participating in the project implementation was less than at the start of the program — 393 offices in 133 localities against over 400 offices collecting bio data in 140 cities as of July 1, 2018.

[30] Central Bank of Russian Federation. URL: http://www.cbr.ru/credit/default.aspx a_115 (accessed: 15.01.2019).

It is important to emphasize that the most systemically important banks, including Sberbank (14 249 offices[31]), Russian Agricultural Bank (1317 offices), Otkrytie Bank (763 offices), etc. do not conduct biometric data collection and do not plan to participate in this project in the future.

To participate in the project, banks should purchase special equipment worth about 4 mln rub. for the first workstation and 130 thousand rub. for each subsequent[32]. For medium and small banks, with the number of branches usually not exceeding 50–100, the total cost will be only about 10–15 mln rub. Large market participants will have to spend more: Alfa Bank will have to spend at least 100 mln rub. However, it is obvious that such expenditures are a "drop in the ocean" for an organization whose assets exceed 3 trln rub. Further, some invested capital will be recovered. In the future, for each successful remote identification, a new servicing bank will have to pay a fee (currently 200 rub.) and some part of which will be transferred to the bank that conducted the initial collection of bio data of the client[33].

In such a situation, an important scientific and applied task is to identify the economic reasons for the poor performance of banks in establishing remote identification. The author identifies three main reasons.

Reason I. Large banks reasonably fear a decrease in their income because of "customer migration". They do not want their wide networks of branches, whose operating costs are truly enormous, to work *de facto* for other banks, attracting new clients for them.

For example, many residents from small villages can pass primary bio-identification, after which they can open accounts in "city" banks and transfer their savings to them. This happens because interest rates on deposits in Sberbank and Russian Agricultural Bank, which have virtually monopolized rural areas, are significantly lower than in many "conventional" commercial banks. With large deposits (up to 1.4 mln rub.) fully insured by the state, state banks are no longer able to secure their key advantage — *a priori* reliability. At the same time, "advanced" urban residents, having submitted bio data in one of the offices of large banks, can then turn to other credit institutions.

To a lesser extent, major banks are concerned about the "migration" of their loan portfolios. Not all retail banks are ready to grant loans to clients who live 300–500 km from their nearest office. (The main reason is that for the case of overdue debts, it can be more complicated to interact with such clients).

Reason II. Many large, medium, and small banks demonstrate little real interest in the transition to remote interaction with clients.

Firstly, there are potential high risks in providing online loans. Currently, only a small number of banks are ready to issue loans "in absentia", i.e. without personal visits by borrowers to bank offices (Sberbank[34], Home Credit[35], etc.). We should note that these banks' effective risk management systems cost them tens of billions of roubles because of bad and

[31] The information on the number of offices is presented hereafter as of 1 December 2018 (Central Bank of Russian Federation. URL: http://www.cbr.ru/credit/default.aspx a_115 (accessed: 15.01.2019)).

[32] Newspaper "Kommersant". URL: https://www.kommersant.ru/doc/3731093 (accessed: 07.02.2019).

[33] Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation № 322 of June 25, 2018. (Matrerials of ConsultantPlus. URL: http://www.consultant.ru/document/cons_doc_LAW_302043/ (accessed: 17.02.2019)).

[34] Sberbank. URL: https://www.sberbank.ru/ru/person/credits/money/consumer_unsecured_fin (accessed: 18.02.2019).

[35] HomeCredit bank. URL: https://www.homecredit.ru/online/credit?fid=0 (accessed: 18.02.2019).

overdue debts written off from their balance sheets. However, most retail banks (Russian Standard[36], OTP-bank[37], etc.), being ready to accept online applications, inform clients only of a preliminary loan decision. Documents must be signed only after personal interview during which a secondary check of client's credit status is performed; based on those results, clients are often denied a loan. Second, banks are doubtful that the option of remote account opening will significantly increase competitive advantages and attract citizens' deposits. Competition in the deposit market is not as intense as in the credit segment at present (there are many money available but few *bona fide* borrowers). However, it does not take much time to open a bank account at a bank's office — usually no more than 20–30 minutes — and the client can perform all further operations remotely via Internet and mobile banking systems.

Third, the Central Bank of the Russian Federation controls whether or not commercial banks comply with Federal Law No. 115–FZ "On countering the legalization of illicit gains (money laundering) and terrorism financing". Any violation thereof, according to Article 20 of Law No. 395–1 "On banks and banking activities", may result in revocation of a bank's license. In this connection, remote account opening can seriously increase risks to banks. For example, currently a bank has no legal grounds to refuse to accept bio data from a citizen who has a passport. For many clients the bank would certainly not open a current account or provide a loan (based on visual screening or after additional verification), but it is still ready to provide "harmless" identification services. Such clients might submit their bio data in one bank and then open accounts in other credit institutions for a fee for shadow bankers.

Reason III. Doubts persist about cybersecurity of the biometric customer identification database generated by banks, and banks are reluctant to become "guinea pigs" when setting up and debugging systems. The cost of an error can amount to billions of rubles and, much worse, to reputational losses that are difficult to remedy.

Solutions. The first problem is to be solved by the Central Bank of the Russian Federation in a purely administrative way (regulatory requirements and fines for non-performance). It is likely that the regulator will prolong the deadlines for commercial banks to join the project, as well as ease the requirements on mandatory biometric equipment at each bank office. The second issue can be resolved only by the *market*. Banks should *recognise* the benefits of their participation in the project. This is unlikely to happen before the third *fundamental* problem of banking cybercrime is solved.

Banking cybercrime as a key factor hindering the development of remote client identification by Russian banks

The media are currently rarely covering topics related to the theft of money in electronic form [Shatalov, 2018]. With cashless payments using bank plastic cards[38] increas-

[36] Bank «Russian standart». URL: https://anketa.rsb.ru/pil/7264/firstWebFormPil (accessed: 18.02.2019).

[37] OTP-Bank. URL: https://www.otpbank.ru/retail/credits/ (accessed: 18.02.2019).

[38] For example, in 2008 89.7 % of transactions performed by individuals using payment cards were related to cashing in ATMs and cash offices of banks. However, in the first half of 2018 the figure reduced almost threefold — to 36.3 %. The remaining ≈⅔ included payments for purchases in stores and transfers between customers (Central Bank of Russian Federation. URL: http://www.cbr.ru/statistics/print.aspx?file=p_sys/sheet014_1.htm&pid=psrf&sid=ITM_48796 (accessed: 21.02.2019)).

ing, there may develop a false sense of complete protection of modern banking Internet technologies against criminal encroachments (Figure 3).

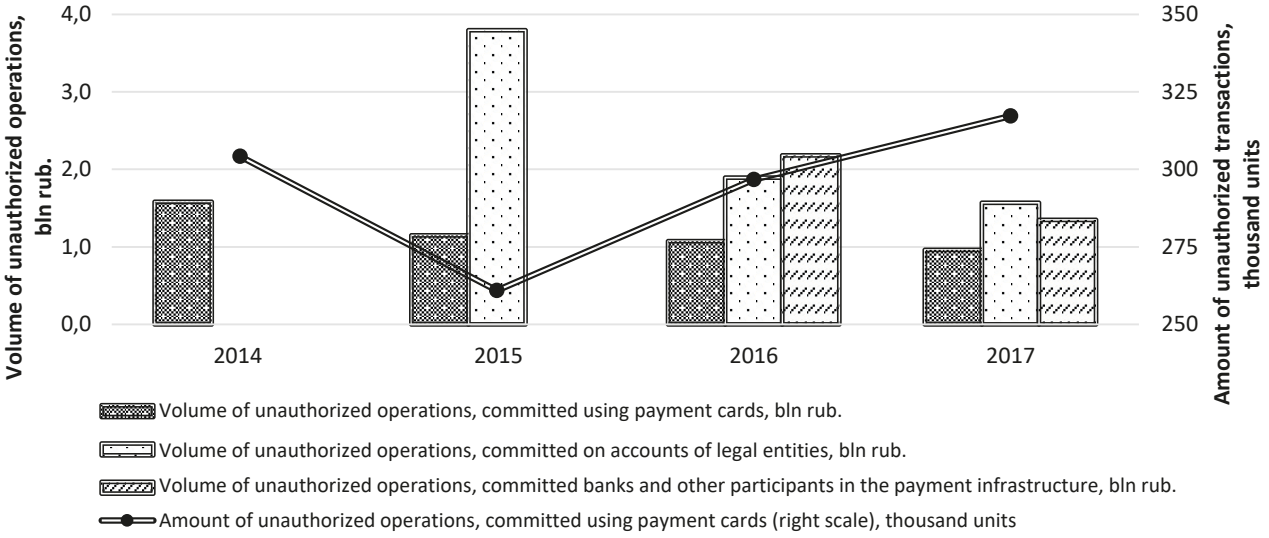

Fig. 3. Information on the number and volume of unauthorized money transfers in Russia in 2014–2017

Note: data for some periods are presented in fragmentary form; data for later periods are absent.

Based on: Central Bank of Russian Federation. URL: http://www.cbr.ru/fincert/ (accessed: 21.02.2019).

As a result of illegal access to "card" accounts, Russians annually lose about 1 bln rub. The number of thefts over the past two years has been increasing almost continuously. For example, in 2017 banks reported 317 thousand unauthorized transfers (almost a thousand cases daily!). It is important to note that the majority of individual losses (75.6 %) occurred during CNP-transactions, i.e. during clearing transactions in the Internet.

RBS (remote banking) systems of enterprises have a higher degree of cryptographic protection than online banking for citizens. They usually use tokens or flash cards, which must be connected to the desktop computer to access the bank account. However, despite this, annual corporate losses consistently exceed those of citizens, amounting to 1.5–2 bln rub. Meanwhile, the number of attempts to obtain illegal access to corporate accounts is much lower than to individual current accounts — 700–800 per year (but as a result, hackers instantly seize large sums, usually between 100 thousand to 10 mln rub.).

Management systems of ATMs, "card" processing centers, and correspondent accounts in other credit institutions and the Central Bank of the Russian Federation obviously have an even higher level of crypto resistance than "conventional" systems. However, as practice shows, they do not provide an absolute guarantee of safety — in the last three years losses exceeded 7 bln rub.!

The key reason for all the above losses is the impact of malicious codes, i.e. the activity of hackers who use special programs to gain unauthorized access to money. More rarely, clients themselves (i.e. voluntarily, but as a result of deception) tell the hackers the information they need to steal money.

There is a variety of legal software in the world used by banks and other companies to run penetration tests on their information systems — Armitage, Cobalt Strike, Empire, and others. As the specialists of the Central Bank of Russia note, they "provide an easy-to-use mechanism for remote management of infected computers… such attacks do not re-

quire special technical knowledge"[39]. The software can be purchased or used free of charge by anyone during the "demo" period. Much less often hackers use genuinely non-standard approaches and original (i.e. their own) programs.

The methods of "social engineering", by which we mean different methods of "tricking out" card numbers, CVC-codes, etc., are not very diverse. They mostly involve phishing: "Your card is blocked, contact the bank's security service", "I'm ready to buy your car (Avito ad, Drom, etc.) and make an advance payment to your card, just tell me the code that you received on your phone", etc.

Thus, both banks and end users are mostly targeted by criminal groups consisting of either "mediocre" programmers or call-centers of "social psychologists". Three articles of the Russian Criminal Code are primarily used to determine and punish cybercriminals (Table 1).

Table 1. **Information on penalties imposed for committing cybercrimes in the Russian Federation**

Article of the Criminal Code of the Russian Federation, paragraph		Description	Penalty	
			Deprivation of freedom	Fine, thousand rub.
Article 158 "Theft"	Par. 3	From the bank account or in relation to electronic money*	Up to 6 years	100–500
	Par. 4	Organised group / especially large scale (≥ 1 mln rub.)	Up to 10 years	–
Article 159.3 "Fraud involving use of payment cards"	Par. 1	Minor damage	Up to 3 years	< 120
	Par. 2	Organised group / considerable damage (≥5 thousand rub.)	Up to 5 years	≤300
	Par. 3	Large scale (≥250 thousand rub.)	Up to 6 years	150–500
	Par. 4	Especially large scale (≥1 mln rub.)	Up to 10 years	–
Article 159.6. "Misappropriation effected via computer systems"	Par. 3	From a bank account or in relation to electronic money	Up to 5 years	150–500
	Par. 4	Especially large scale (≥1 mln rub.)	Up to 10 years	–

Note: * including by illegal entry into a home, from an oil pipeline, etc.; the amount of fine as an independent type of penalty; a dash means "not provided"; par. — paragraph.

Based on: Article 21 of the Civil Code of the Russian Federation (Materials of ConsultantPlus. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (accessed: 20.02.2020)).

According to an explanation provided by the Supreme Court of the Russian Federation, most crimes that involve larceny of money from bank accounts are classified as theft. Unlike fraud, theft (under Article 158 of the Criminal Code of the Russian Federation) implies stealing money by criminals if they obtained a client's login/password or card number and CVC-code from a client-bank system by means of deception or breach of trust and then stole the money. This is because "deception is not directly aimed at seizing someone else's property, but is only used to facilitate access to it"[40].

[39] Main types of cyber attacks against the financial sector (The Overview of the Central Bank of the Russian Federation) Central Bank of Russian Federation. URL. http://www.cbr.ru/StaticHtml/File/14435/gubzi_17.pdf (accessed: 24.02.2019).

[40] On the judicial practice in cases of fraud, misappropriation and embezzlement: Resolution of the Plenum of the Supreme Court of the Russian Federation of 30.11.2017, No. 48 (Materials of ConsultantPlus. URL. http://www.consultant.ru/document/cons_doc_LAW_283918/ (accessed: 28.02.2019)).

Article 159.3 of the Civil Code of the Russian Federation applies when theft of property was committed by personally presenting stolen or forged payment cards to the cashier of a bank or a shop (if money was illegally withdrawn at an ATM, such act is qualified as theft). This article, as well as the Article 159.6[41] on misappropriation effected via computer systems, is used quite rarely in Russia (Table 2).

Table 2. **The number of people convicted in Russia under specific articles of the Criminal Code in 2012–2018**

Article	2012	2013	2014	2015	2016	2017	2018*
Article 159.6 (p. 3–4)	–	20	19	16	35	62	36
Article 159.3	–	259	251	154	84	79	94
For reference							
Article 159.6 (part. 1–2)	–	39	59	72	89	82	30
Article 159	23 649	19 669	18 033	17 690	17 644	17 757	16 544
Article 158	224 268	213 809	198 990	209 611	199 077	175 390	162 690

Note: * — data for 2018 is obtained by means of doubling the data for the 1st half year.

Based on: Judicial Department of the Supreme Court of the Russian Federation. URL: http://www.cdep.ru/index.php?id=79 (accessed: 28.02.2019).

Apparently, the state is much more active in exposing and punishing "common" thieves and fraudsters (Articles 158 and 159). The number of "hackers" convicted annually on a national scale is insignificant, ranging from 20 to 50 (all trials ending in convictions). However, there are even fewer cases involving "bank hackers", since: a) almost all of them are convicted as accomplices; b) under paragraphs 3 and 4 of Article 158.6 they are convicted of "hacking" not only banking, but also other types of information systems. It should be noted that the real penalties for such crimes are rather lenient (Table 3).

Table 3. **Types of penalties for the offenders convicted under paragraphs 3 and 4 of Article 159.6 of the Criminal Code of the Russian Federation in 2017–2018**

Type of penalty / Paragraph of Article 159.6 / Year	Paragraph 3		Paragraph 4	
	2017	6 months of 2018	2017	6 months of 2018
Deprivation of freedom	5	–	25	6
Suspended sentence	9	7	17	3
Correctional works	–	–	–	–
Fine	6	1	–	–
Amnesty	–	1	–	–
Total	20	9	42	9

Note: a dash means "not provided".

Based on: Judicial Department of the Supreme Court of the Russian Federation. URL: http://www.cdep.ru/index.php?id=79 (accessed: 28.02.2019).

[41] The common schemes of such crimes as "creation of fake sites of charity organizations and online stores" are regulated by the Article 159 "Fraud". Even though both Articles 159 and 159.6 establish the same maximum penalty (up to 10 years of imprisonment), the criteria for determining the amount of damage differ significantly. For example, in the first case especially large scale damage is the damage exceeding 12 mln rub., while in the second case it amounts to "only" 1 mln rub.

In practice, in 2018 courts usually imposed a suspended sentence or a fine (5 to 300 thousand rub.) for fraudulent actions that resulted in damage of up to 1 mln rub. (par. 3 of Article 159.6). Moreover, in 40 % (!) of cases the criminals were given a suspended sentence even under par. 4[42]. The duration of effective imprisonment was usually between 2 and 5 years.

Based on the above, it is possible to draw the following conclusions. *First*, Russian criminal legislation is somewhat "confusing" with cybercrime being "scattered" under various articles of the Criminal Code of the Russian Federation, and their paragraphs regulate not only bank crimes. The latter makes it significantly more difficult to use statistics[43] to analyse the impact of punishment on "ordinary" fraudsters and thieves, as well as bank hackers. *Second*, the number of cases involving bank hackers that have been brought to court is extremely low. However, it is their "activities" that are most dangerous for the advancement of e-banking services. *Third,* the courts rarely hear cases related to uncompleted crimes (preparation or attempt). This is probably due to victims' reluctance to appeal to competent authorities when hackers failed to steal money from them. *Fourth*, the courts are taking a very lenient attitude towards computer criminals. As a result, most of offenders escape any significant punishment.

In author's opinion, the results of the government efforts to combat cybercrime in the Russian banking sector can hardly be considered satisfactory. This significantly hinders the development of modern Internet technologies in banking, including the innovative system of remote customer identification.

Key problems in the development of remote client identification in the Russian banking system and their solutions

Problem I. The risk of unauthorized access to the Unified Biometric System, which may result in: a) disclosure of clients' personal data to the public (at least in the Internet, Tor, darknet); b) use of accumulated biometric data for banking operations by unauthorized persons (criminals). It is important to note that compromised biometric data, unlike lost logins, passwords, certificates, PIN codes, etc., cannot be recovered!

Solution. Taking into account the devastating consequences of the above, it is essential to conduct a lengthy pilot operation of the system (Chinese experience). As the project has already been launched in Russia and there is no "turning back" without reputation losses, the Central Bank of the Russian Federation should not put too much pressure on the banking community (taking into account the Indian experience).

Problem II. Concerns of a large number of citizens regarding breach of their privacy. Thus, according to Article 14.1 of the Federal Law No. 149–FZ "On Information…" Rostelecom, as an UBS operator, is obliged to provide information stored in a unified biomet-

[42] It is impossible not to mention that the number of people who recieved a suspended sentence under paragraph 1 of Article 158 applied to those who "stole a sack of potatos" in the first 6 months of 2018 was approximately the same as the number of hackers, who inflicted damage in a particularly large amount — 44 %. The question is whether this is fair.

[43] Unfortunately, statistics of the Ministry of Internal Affairs in this matter are much less informative than the materials of the Judicial Department of the Supreme Court of the Russian Federation, which were used in this work.

ric database upon the request of the Ministry of Internal Affairs and the Russian Federal Security Service.

Solution. An increased liability for the unauthorised use of information from the UBS, together with explanatory and educational activities to reduce social tension. Meanwhile, law-abiding citizens obviously have nothing to fear under the primacy of the rule of law.

Problem III. Lack of transparancy regarding the proper testing of the UBS software, developer's and operator's guarantees, etc. This significantly reduces the confidence of potential users (both banks and citizens) in the project. For example, "requirements to biometric data (face image and voice recording)…" posted on the Rostelecom portal, contain a bibliographic list, which includes six works by foreign scholars. This should probably increase confidence in the document and the system as a whole. However, all these articles are related to the study of voice biometrics [Beigi, 2011; Barinov, 2010; Pearce, 2000].

Solution. Rostelecom, as an EBS operator, should publish on its website: a) technical specifications of the systems; b) a positive opinion of an authoritative research institute or university including an analysis of relevant studies (rather than 20-year-old materials) by leading Russian and foreign scholars; c) a series of popular scientific video that would demonstrate the reliability and convenience of the system.

Problem IV. The risk of unauthorized access to the UBS system by unauthorized persons who successfully completed the identification procedures. There is no publicly available information about the probability of a false matches in the UBS. However, the specifications attached to the tender documentation allow 0.1 % probability of a false coincidence in the UBS[44]. So, a computer may make a mistake once in a thousand matches. This error value may indeed seem small, but the Amazon American platform, for example, with photos of 25 000 criminals uploaded, has "identified" 28 of them among the current congressmen[45]. It would appear that the error in this case was only a minor 0.112 %. However, there are implications for this "statistical error"! Besides, repeated experiments on the most perfect gadgets confirm that, despite scanning "30 thousand dots and eyes"[46], twins can easily unlock the bio identification system. Similar results were obtained using high-precision human face masks[47].

In fact, any biometric recognition system has a problem with setting the degree of "accuracy". If the algorithm is made very "rigid", then with decreasing the probability of second-generation error (acceptance of a false match, which was discussed above), the probability of first-generation error will increase (deviation of the correct match). In other words, the users will have problems accessing the system (according to the technical specifications, the probability of false mismatch of the UBS is 3 %).

Solution 1. It is obvious that modern biometric technologies designed for large-scale application cannot guarantee a high level of reliability (which must be a priority, since we are talking about people's savings). New customers must be additionally identified by:

---

[44] D-Russia. URL: http://d-russia.ru/wp-content/uploads/2017/06/TZ-biometriya.pdf (accessed: 14.02.2019).

[45] CNET. URL: https://www.cnet.com/news/amazon-facial-recognition-thinks-28-congressmen-look-like-known-criminals-at-default-settings/ (accessed: 14.02.2019).

[46] Iguides. URL: https://www.iguides.ru/main/security/bliznetsy_i_iphone_x_udastsya_li_obmanut_face_id/ (accessed: 22.02.2019).

[47] Macdigger. URL: https://www.macdigger.ru/news/post/face-id-obmanuli-s-pomoshhyu-3d-maski (accessed: 22.02.2019).

a) confirming one-time passwords from a previously registered mobile phone number[48]; b) entering a secret code word. Besides, in order to reduce the risk of forced identification (under threat), it is necessary to foresee the possibility of using a combination of words, after which the system will be blocked until a personal visit to the bank (the system then should a loss of connection or other technical problem).

Solution 2. In fact: a) there is no information about the real capacity of the bioidentification system; b) the number of bioidentification procedures is by no means unlimited[49]. Therefore, it is necessary (at least at the first stages) to conduct bioidentification under the control of the employees of the bank where the client wants to open an account. This follows the Austrian and Swiss experience and will: a) prevent the violation of Federal Law No. 115–FZ; b) detect and correct the existing defects in the new system; c) increase the credibility of the project for both the banks and the potential clients.

Solution 3. It is necessary to introduce a mandatory periodic prolongation of citizens' consent (every 3–5 years) to the use of biometric templates, carried out in person at bank offices (following the experience of South Korea).

Problem V. At present, the client himself bears the responsibility for unauthorized access to the UBS system, as he signs a written statement of consent specifying the relevant risks. At the same time, the bioidentification process is not subject to video recording and storage. In this case it is very difficult (in fact, almost impossible) for the client to prove his innocence during an investigation and in court.

Solution 1. All bioidentification procedures should be video recorded and stored for a period of 3–5 years; they should be made available upon request of the competent authorities in the investigation of theft and fraud in the banking sector (Austrian experience).

Solution 2. Rostelecom, as the UBS operator, should create a special fund to compensate clients for the unauthorized use of customer records. The funds should be generated by Rostelecom itself and the banks that want to use bio identification for new clients.

Problem VI. The current efforts to combat cybercrime in the banking sector consist mainly in "rebuffing" cyber attacks. In the event of actual theft, neither banks nor their clients would normally report it to law enforcement agencies. Moreover, banks are not authorized to report such crimes if the subject of theft is clients' money (as formally they are not victims). The government, in fact, remains unaware of the majority of crimes committed, and therefore such crimes are not investigated at all.

Solution 1. Banks should be obliged to report to law enforcement agencies no matter how successful the hackers' attacks have been[50]. To form a complete picture of computer crime, banks should be allowed to accept statements from their clients about thefts to forward the information for further investigation to the law enforcement agencies.

Solution 2. Establishing specialized departments to investigate cybercrimes in the banking sphere. It would be sensible to study the UK experience. Since 2017, Financial Fraud Action UK, consisting of about 300 financial institutions and banks, has been fund-

[48] There are certain problems associated with the illegal reissue of SIM cards of mobile operators in this area. However, this is the subject of a separate study.

[49] Customers pass it once during initial identification at the bank. Otherwise, the bank will have to pay 200 rubles for each client's entry into "Internet Banking" system which is too expensive. Therefore, customers will need to be identified biometrically only once ("at login") and then will use "traditional" logins and passwords from "regular" Internet Bank system.

[50] The uncompleted act (attempt or preparation) constitutes an offence.

ing a special police department to investigate cybercrimes connected with illegal card transactions[51].

Problem VII. In modern Russia, cybercriminals remain either unpunished or the court imposes fairly lenient penalties (fines, suspended sentence).

Solution. Legislative and judicial authorities should pay attention to the serious public threats posed by high-tech fraud in electronic banking information. Indeed, the district courts are full of young people (usually not older than 30 years) who committed a faux pas, rather than hardened criminals. Yet in most cases, the courts deliver minor or suspended sentences for the established offence, and never impose correctional or compulsory work (Table 3).

General risks of global digitalization in the process of developing the institute of remote biometric identification in Russian banks

The rapid technological development that took place at the beginning of the 21st century, resulting from digitalization of virtually all sectors of the economy, is, according to many scholars, "a key element of the fourth industrial revolution" [Rihter, Pahomova, 2018]. The level of digitization of the financial and banking sector is constantly growing [Belousov, Levchuk, 2018]. Despite obvious advantages, this also increases operational and other risks for banks. For example, the author distinguishes three main groups of economic risks resulting from the introduction of biometric remote client identification initiated by the Central Bank of the Russian Federation.

Group I. Risks related to inaccurate functioning of the remote identification system, which lead to direct and indirect material losses of clients and/or banks, as well as reputational losses incurred by credit institutions, operators and vendors of the newly created Unified Biometric System.

Group II. Negative impact on the development of the Russian financial and banking system due to significant and unorganized changes in its existing structure. The expantion of remote interaction with clients may significantly weaken the competitive position of a large number of domestic banks, especially medium and small ones, which, due to limited financial resources, will not be able to fully integrate their business into the new digital model of interaction with customers. Despite the fact that this risk is generally market related, it may lead to certain destabilization of the domestic banking system in the medium term due to disorderly exit of a number of uncompetitive banks from the market (as it happened in the Russian banking system earlier).

Group III. Social and economic risks associated with a significant reduction in the number of bank employees engaged in direct interaction with clients. It should be noted that these risks are among the general risks of the fourth industrial revolution which is expected to replace low- and medium-skilled specialists with artificial intelligence [Maslov, Luk'yanov, 2017].

Regulation of the above risks (in order to minimize negative economic and socio-economic consequences) is only possible if the institute of remote client identification in the domestic banking system is operational. Therefore, they should be taken into account

[51] Financial Fraud Action UK. URL: https://www.financialfraudaction.org.uk/police/ (accessed: 24.02.2019).

when adopting regulatory measures in the relevant area in the future — both in the medium- and long-term perspective.

Conclusion

The analysis of scholarly literature, as well as the global experience of developed and developing countries, demonstrates convincingly the advantages of the national institutions of remote client identification by banks. However, their technological characteristics differ significantly. Foreign countries employ different approaches combining biometric and non-biometric methods (online video identification, use of traditional logins/passwords, etc.). In Russia, the Central Bank of Russia initiated the creation of the national institute of remote biometric client identification using photo and audio templates of citizens collected on a centralized basis. Despite the fact that similar opportunities were provided to commercial banks on July 1, 2018, de facto they do not take an active part in the innovation project. There are two groups of reasons explaining this fact: lack of economic motivation and unwillingness of clients (individuals) to submit biometric data on a voluntary basis. It should be emphasized that these reasons (which have been described in detail above) are objective in nature. The author has also identified seven main groups of key problems that hinder the systemic development of the institute of remote identification of clients in the Russian banking system, provided practical recommendations to address them in the short and medium term, and outlined a number of common risks that global digitalization poses for the establishment of an innovation institute in Russia for the purpose of overcoming economic and social problems. This made it possible to confirm the correctness of the originally formulated scientific hypothesis, as well as to achieve the goal of scientific research and fulfil all the tasks set within it.

Implementation of the project on remote client identification in the Russian banking system is, undoubtedly, a step in the right direction. A new generation of clients is already prepared for new and unconventional communication technologies. However, to reach real positive potential of the bioidentification system, it is necessary to pay attention to objective problems in this area. If they are ignored (as is currently the case), direct losses, reputational losses, and lack of credibility among the population and banks can literally "bury" this undoubtedly ambitious and innovative social and economic institution in Russia.

Acknowledgment

The author is grateful to anonymous reviewers for useful suggestions and recommendations, which made it possible to strengthen and generalize the arguments, expand the bibliographic analysis, and generally improve the quality of the text.

References

Awad A. (2016) From classical methods to animal biometrics: a review on cattle identification and tracking. *Computers and Electronics in Agriculture*. Amsterdam, Elsevier Science Publishers B. V., pp. 423–435.

Banerjee S. (2015) From cash to digital transfers in India: The story so far. *Customer-Centricity for Financial Inclusion brief*. Washington, DC, World Bank, pp. 1–4.

Barinov A. (2010) *Voice samples recording and speech quality assessment for forensic and automatic speaker identification. 129th Audio Engineering Society Convention*. San Francisco, AES, pp. 334–343.

Beigi H. (2011) *Fundamentals of Speaker Recognition*. Yorktown Heights, Springer. 909 p.

Belousov A. L., Levchuk E. Yu. (2018) Didzhitalizatsiia bankovskogo sektora. *Finansy i kredit*, vol. 24, no. 2 (770), pp. 455–464. (In Russian)
Chajkina E. V., Kozinkin A. A., Chajkin V. Yu. (2018) Innovative technologies as a factor of competition in the Russian banking market. *Nauchnyi vestnik: finansy, banki, investitsii*, no. 4, pp. 114–121. (In Russian)
Charles A. (2018) Biometrics, the future of banking and financial service industry in Nigeria. *Journal of Electronics u Information Engineering*, vol. 9, no. 2, pp. 91–105.
Dostov V. L., Shust P. M., Kozyreva A. D. (2017) New concepts of applying a risk-based approach in the implementation of identification procedures. *Iuridicheskaia nauka*, no. 5, pp. 104–112. (In Russian)
Emets M. I. (2019) Remote identification of bank customers: prospects and challenges for compliance services. *Mezhdunarodnaia nauchno-prakticheskaia konferentsia mezhdunarodnogo setevogo instituta Epokha kriptoekonomiki: novye vyzovy*. Moscow, Publishing House of the MIFI, pp. 231–237. (In Russian)
Gelb A., Decker C. (2011) Cash at Your Fingertips: Biometric Technology for Transfers in Resource. *CGD.* Washington, D. C., Center for Global Development, pp. 1–43.
Indrayani E. (2014) The Effectiveness and the Efficiency of the Use of Biometric Systems in Supporting National Database Based on Single ID Card Number. *Journal of Information and Software Technology*, vol. 4, no. 1, pp. 129–138.
Khan A. (2018) National Identity Card: Opportunities and Threats. *Journal of Asian Research*, vol. 2, no. 2, pp. 77–85.
Kozlova N. P., Ustinova E. V. (2019) Digitization of the banking sector: trends and cases of development of the Russian market. *Ekonomika. Biznes. Banki*, no. 1, pp. 18–34. (In Russian)
Krivoruchko S. V., Maklakova T. R. (2017) World practice of development of biometrics in the provision of payment services to increase their accessibility. *Uchenye zapiski Rossiiskoi akademii predprinimatel'stva*, vol. 16, no. 4, pp. 184–192. (In Russian)
Krivoruchko S. V., Ponomarenko V. Ye., Lopatin V. A. (2019) *Increasing the availability of payment services through the development of user identification systems.* Moscow, Infra-M Publ. 157 p. (In Russian)
Krylova I. Yu., Rudakova O. S. (2018) Biometric technologies as a mechanism for ensuring information security in the digital economy. *Molodoi uchenyi*, no. 45 (231), pp. 74–79. (In Russian)
Kumar S. (2019) *Cattle Recognition: A New Frontier in Visual Animal Biometrics Research. Proceedings of the National Academy of Sciences*. Ed. by Jai Pal Mittal. Deli, Springer, pp. 241–248.
Lozhnikov P. S. (2017) *Biometric protection of hybrid workflow: a monograph*. Novosibirsk, Publishing House of the SB RAS, 2017. (In Russian)
Martens A. A. (2018) Remote maintenance as a basic technology for the development of banking business. *Lizing*, no. 6, pp. 39–44. (In Russian)
Martin A. (2012) National Identity Infrastructures: Lessons from the United Kingdom. *10th International Conference on Human Choice and Computers (HCC)*. Amsterdam, Springer, pp. 44–55.
Maslov V. I., Luk'yanov I. V. (2017) The fourth industrial revolution: sources and consequences. *Vestnik Moskovskogo universiteta. Seriia 27: Globalistika i geopolitika*, no. 2. pp. 38–48. (In Russian)
Medvedeva E. A. (2018) On the prospects for the development of remote customer identification. *Bankovskoe delo*, no. 12, pp. 59–61. (In Russian)
Naumov V. (2018) Problems of development of legislation on identification of the subjects of information space in digital economy. *Trudy Instituta gosudarstva i prava RAN*, vol. 13, no. 4, pp. 125–150.
Nazarov S. V. (2018) Electronic documents and remote identification of individuals. *Dnevnik nauki*. no. 6 (18), pp. 34-41. (In Russian)
Pearce D. (2000) Enabling New Speech Driven Services for Mobile Devices: An overview of the ETSI standards activities for Distributed Speech Recognition Front-ends. *The Speech Applications Conference*, San Jose, Motorolla Lab., pp. 1–11.
Rihter K. K., Pahomova N. V. (2018) Digital economy as an innovation of the XXI century: challenges and chances for sustainable development. *Problemy sovremennoi ekonomiki*, no. 2. pp. 22–31. (In Russian)
Shatalov A. S. (2018) Phenomenology of crimes related to the use of modern information technologies. *Zhurnal Vysshei shkoly ekonomiki*, no. 2, pp. 68–83. (In Russian)
Shnekutis S., Gobareva Ya. (2018) Remote identification and biometrics in the field of remote banking services. *Khronoekonomika*, no. 1, pp. 67–71. (In Russian)
Vengerovskij E. L. (2018) Innovatsii internet-bankinga kak faktor konkurentosposobnosti kreditnykh organizatsii na sovremennom rynke bankovskikh uslug. *Bankovskoe pravo*, no 5, pp. 47–52. (In Russian)
Yakimenko A. A., Vikhman V. V. (2016) *The introduction of biometric identification in access control systems*. Novosibirsk, Publishing House of the NSTU. 54 p. (In Russian)

Received: 17.05.2019
Accepted: 20.02.2020

Author's information:

Yurii S. Ezrokh — Dr. Sci. in Economics, Associate Professor; ezroh@rambler.ru

Проблемы становления института удаленной идентификации клиентов в российской банковской системе (экономические аспекты)

Ю. С. Эзрох

Новосибирский государственный университет экономики и управления,
Российская Федерация, 630099, Новосибирск, ул. Каменская, 56

Для цитирования: Ezrokh Y. S. (2020) Problems of establishing the practice of remote identification of clients in the Russian banking system (economic aspects). *Вестник Санкт-Петербургского университета. Экономика*. Т. 36. Вып. 2. С. 266–286.
https://doi.org/10.21638/spbu05.2020.205

Статья посвящена анализу экономических аспектов становления в России института удаленной идентификации кредитными организациями своих клиентов, целесообразность развития которого обусловлена перманентной диджитализацией модели взаимодействия субъектов банковских отношений. В работе представлены результаты анализа экономических аспектов функционирования удаленной идентификации банками своих клиентов в развитых и развивающихся зарубежных странах (Австрии, Великобритании, Индии, Китае, США, Швеции, Швейцарии и Южной Корее), раскрыты теоретические и практические особенности функционирования системы банковской биометрической идентификации в России на современном этапе. На основании комплексного анализа сформулированы экономические причины отсутствия мотивации у большинства отечественных банков в развитии нового института. Впервые в российской экономической литературе в систематизированном виде раскрыты ключевые проблемы, являющиеся сдерживающими факторами развития института удаленной идентификации клиентов в России: а) риск несанкционированного доступа к центральному хранилищу данных; б) опасения относительно нарушения приватности частной жизни; в) отсутствие в свободном доступе материалов об апробации программного обеспечения, гарантиях компаний-разработчика, оператора и т. д.; г) риск получения несанкционированного доступа к Единой биометрической системе путем успешного прохождения идентификационных процедур посторонними; д) риск финансовых убытков от несанкционированного доступа к данной системе, переложенный на клиентов; е) неудовлетворительные результаты борьбы с банковской киберпреступностью в России. Автором представлен ряд научно обоснованных предложений по преодолению указанных проблем и минимизации экономических рисков использования системы удаленной идентификации клиентов в России с учетом позитивного и негативного опыта, накопленного за рубежом.

Ключевые слова: биометрия, видео-идентификация, Единая биометрическая система, идентификация клиента, киберпреступление, онлайн-идентификация, финтех, экономические риски удаленной идентификации.

Статья поступила в редакцию: 17.05.2019
Статья рекомендована в печать: 20.02.2020

Контактная информация:

Эзрох Юрий Семенович — д-р экон. наук, доц.; ezroh@rambler.ru