EQUILIBRIUM
Quarterly Journal of Economics and Economic Policy
2017 VOLUME 12 ISSUE 3, September
p-ISSN 1689-765X, e-ISSN 2353-3293
www.economic-policy.pl

ORIGINAL PAPER

Citation: Piotrowska, A. I., Polasik, M., & Piotrowski, D. (2017). Prospects for the application of biometrics in the Polish banking sector. *Equilibrium. Quarterly Journal of Economics and Economic Policy*, *12*(3), 501–518. doi: 10.24136/eq.v12i3.27

Contact to corresponding author: michal.polasik@umk.pl, Nicolaus Copernicus University in Torun, ul. Gagarina 13a, 87-100 Toruń, Poland
Received: 13 April 2017; Revised: 4 June 2017; Accepted: 19 June 2017

Anna Iwona Piotrowska
Nicolaus Copernicus University in Torun, Poland

Michał Polasik
Nicolaus Copernicus University in Torun, Poland

Dariusz Piotrowski
Nicolaus Copernicus University in Torun, Poland

Prospects for the application of biometrics in the Polish banking sector

JEL Classification: *E42; G21; G28; O33*

Keywords: *biometric; payment system; banking sector*

Abstract
Research background: The ongoing digitisation process in the banking sector, coupled with widespread remote provision of services, is leading to the advent of new solutions in the field of broadly understood security. The increasingly sophisticated forms of attacks on banks' IT systems and their users have engendered the need to implement authentication methods that would ensure high security levels, but would also be convenient for banks' clients and suited to the requirements of mass service. Biometric technology seems to be a solution to this issue. The two factors that may boost its proliferation are: the fact that banks need to adjust to more rigid regulations, and technological advancements leading to cost reduction and increased availability of biometric solutions in mobile devices.
Purpose of the article: The purpose of the article is to assess the prospects for the application of biometrics by the banking sector in Poland in individual customer service channels.
Methods: The basis for theoretical considerations comprises the analysis of literature on authentication techniques and research on the processes whereby consumers accept new technologies. The empirical part of the paper was based on the results of the authors' questionnaire survey among representatives of the Polish banking sector.

Findings & Value added: The banking sector in Poland is on the verge of a sweeping biometric revolution in the coming years, because most traditional identity verification and authorisation methods currently available in banking do not comply with strict security and user convenience requirements and RTS regulations. Biometric technologies will be of use in all customer service channels, with the experts indicating authentication in bank branches, ATMs, and mobile banking as the primary implementation areas. Solutions which are most likely to be applied are those based on biometrics of fingerprints and finger veins, as well as voice biometrics.

Introduction

In the modern economy, based on the functioning of IT systems collecting and processing data in the form of digital records and the mass provision of services through electronic channels, the issue of ensuring adequate security levels is becoming a pivotal challenge. This stems from the unsought effect of technological advancements, namely the development of cybercrime manifested in new types of attacks, tools and techniques allowing attackers to penetrate even well-controlled environments (Bendovschi, 2015). The phenomenon's scale is depicted in the results of a study conducted in 2015 and commissioned by the UK government where 90% of large entities in different British industries reported that the security of their IT systems had been compromised in the year preceding the survey (HM Government, 2015). The financial sector, and the banking sector in particular, is very susceptible to cyber-attacks, which may potentially put financial stability at risk by interfering with the primary functions performed by the financial system in the economy (Bank of England, 2015). The need to ensure public trust in financial institutions is driving governments and companies to intensify their efforts aimed at boosting the security of services provided electronically. Although there has been some progress in developing the resistance of financial institutions to cyber-attacks, the risk of their appearance is constantly growing (Bank of England, 2017).

For several decades now, high hopes have rested in biometrics as a tool to raise security levels in the financial sector while ensuring a high degree of convenience[1]. The banking sector is particularly interested in this type of solution (Venkatraman & Delpachitra, 2008). Until now, however, the extent to which biometrics have been implemented by both Polish and European institutions has been very limited. The purpose of the article is to assess the prospects for the application of biometrics by the banking sector in Poland in individual customer service channels.

[1] According to Seiders *et al.* (2007), transaction convenience refers to how customers perceive the time and effort of finalising the transaction.

The article is divided into two main parts. The first part presents a critical analysis of the literature on the subject, containing a discussion on the significance of security and convenience for consumers' use of online banking services and pointing out the main types of biometric solutions applied in banking. The second part presents the results of a questionnaire survey among experts from the Polish payment services sector. The analysis also takes into account the potential impact of the Regulatory Technical Standards (RTS), issued by the European Banking Authority (EBA) in its implementation of Payment Services Directive 2 (PSD2), on banks' interest in using biometrics in payment services.

The significance of security and convenience for consumers' use of online banking services

In literature, there are many theoretical models describing the process whereby users except financial innovations. According to Zhu & Chang (2014), the most widespread model in the study of information technology adoption is the Technology Acceptance Model (TAM) and its many subsequent extensions (Lancelot Miltgen *et al.*, 2013; Venkatesh *et al*., 2003). These models indicate that both key constructs of TAM, i.e. perceived utility and perceived ease of use of a given innovation, are pivotal for explaining the financial and payment services acceptance process (Kim *et al*., 2010; Polasik *et al.*, 2012; Schierz *et al.*, 2010; Shin, 2009). It is worth noting that the variable 'convenience' is an important component with an effect on the materiality of both perceived utility and perceived ease of use of many innovations (Kim *et al*., 2010). It was directly applied in other empirical studies (Aliy *et al.*, 2012; Koulayev *et al.*, 2016).

Previous research of the authors has indicated that the sense of security is of paramount importance for the practical use of online banking by customers (Polasik & Wisniewski, 2009). The works of other authors also point to the extremely important role of the sense of security in consumers' decision to use online banking and mobile payments (Aliyu *et al*., 2012; Koulayev *et al*., 2016; Shin, 2009). In turn, according to Casaló, Flavián, & Guinalíu (2007) consumer-perceived security of the management of their personal data has a direct and positive effect on trust in online financial services. It should be emphasized that the reputation plays an important role in customer loyalty (Szwajca, 2016), and the process of innovativeness has strong impact on the banking sector (Kubiszewska, 2017).

The abovementioned key role of two factors, security and convenience, led the authors to adopt a 'convenience versus security' approach, which

was successfully applied by Shen *et al.* (2010) to explain the consumer adoption of the mobile banking system. Within that perspective it is assumed that the key benefit of a banking solution is convenience, while the key disincentive is the effort of dealing with security system (Shen *et al*., 2010). Therefore, the paper opted for convenience offered to customers and the level of security as the starting point for the analysis of authorisation methods which may be applied in mobile banking.

The nature and types of biometric solutions applied in banking

The term 'biometrics' takes its roots from ancient Greek words: *bios* —— life, and *metron* — measure (Sahoo *et al.*, 2012). Biometrics is a technology used to measure and analyse biometric data (Malathi & Jeberson Retna Raj, 2016), i.e. predominantly physical or behavioural human identifiers (Lumini & Nanni, 2017), and less frequently chemical identifiers (Pocovnicu, 2009). The biometrics based on physical features comprise the analysis of data regarding face or palm shape, fingerprints, the iris or the arrangement of blood vessels. Physiological biometrics is related to the shape of the body and is generally more stable, e.g. fingerprint, iris, retina, hand geometry and vein geometry. Behavioural features are generally less stable over time than physical ones, and they include primarily speech, signature, or keystroke dynamic (Sahoo *et al*., 2012). Lastly, chemical identifiers relate to body odour and heat (Pocovnicu, 2009).

The literature prevalently indicates that it is possible to practically apply biometric data which have the following characteristics (Gaikwad & Pasalkar, 2004; Khandelwal *et al.*, 2016; Kumar & Farik, 2016):

- Universality. Practically all people are a source of such data, except for those with congenital defects or disabilities acquired throughout life.
- Distinctiveness. Each person has unique characteristics absent in others.
- Permanence. Features ascribed to an individual remain unaltered or undergo very slight changes during the lifetime of their bearer.
- Collectability. Individual characteristics may be collected and processed into digital records.

Biometric data are used in the authentication process. Authentication is a technique that a computer system uses to verify the identity of a person who seeks to access the resources of that system (Kumar & Farik, 2016). Biometrics is a separate group within the three types of methods used to identify and authenticate consumers in banking (Deloitte, 2017; Matyas & Rilla, 2002):

- methods based on "something I know", e.g. password, PIN,
- methods based on "something I have", e.g. identity document, token,
- methods based on "who I am" (biometric features), e.g. fingerprint.

Identification and verification grounded in biometric technologies is entirely different from traditional methods, because the authentication process uses unique physical traits. Therefore, it may only be carried out if the user allows biomedical data to be read. With biometric technologies, there is no need to memorise passwords or hold an identity-verifying document — biometric credentials cannot be stolen, lost, forgotten or guessed (Lumini & Nanni, 2017; Pocovnicu, 2009). They require, however, adjusted technical equipment and the consent of the user to provide samples of their biometric data. The use of this technology raises a number of technological and ethical issues, mostly privacy concerns associated with data storage and the individual right to privacy (Alterman, 2003; Bustard, 2015; Van der Ploeg, 2003).

The functioning of biometric systems involves two phases: the enrolment phase and the identification and verification phase. Firstly, biometric data is acquired by a sensor module. The process should take a form acceptable for the identified person, while measurements ought to be fast and accurate. Then, the collected 'live sample' of the user is processed and stored as a template. In the verification process, captured biometric data are compared against the enrolled template. The authentication process ends with the acceptance or rejection of the claimed identity (Lumini & Nanni, 2017). These features of the biometric system point to considerable technical challenges related to the use of biometrics on a mass scale.

Due to the fact that financial services are provided in a specific manner, the paper narrows down the analysis to selected biometric techniques used or with a large potential to be used in the banking sector. Table 1 presents their main features.

It should be underscored that there is no single ideal and universal biometric technique. Each solution has its advantages and disadvantages which determine whether it may be used in particular areas (Khandelwal *et al*., 2016). What can prove to be a partial answer to the issue of seeking the ideal solution is biometric system fusion (Jagadiswary & Saraswady, 2016; Lumini & Nanni, 2017).

Research methodology

In order to achieve the purpose of the paper, it was fundamental to conduct an analysis based on selected results of the survey among representatives of

financial institutions operating in Poland. The survey was carried out between June and December 2014 as part of a research project of the Warsaw Institute of Banking and ALTERUM Grant No. WIB/2014/01, "Growth through innovation or economies of scale? Survey of the participants of the Polish payment system" (Polasik *et al.*, 2015). The study was addressed to 470 experts selected by the Polish Bank Association dealing with innovation in the payment services market within the surveyed institutions. Responses were provided by 70 experts (response rate of 15%), however due to the fact that there was no obligation to answer all the inquiries, the sample size differs among particular questions. Experts represented the most important types of institutions functioning in the payment services market in Poland, namely commercial banks (almost 40%), institutions processing and settling payment transactions (23%), IT companies providing solutions for the payments sector (17%), banking institutions, card associations and cooperative banks. Figure 1 presents information regarding the respondents indicating their high competence and decision-making powers. The results were analysed using the PS IMAGO/SPSS statistical software package. This demonstrates the high cognitive value of the obtained empirical results.

Anticipated prospects for the application of biometrics in the banking sector in Poland

To date, the scope of biometrics implementation is limited both in the Polish and the European banking system. Polish cooperative banks were trailblazers in that respect on the European scale, as they introduced biometric ATMs with finger vein technology in 2010. In 2012, Bank BPH was the first in Europe to implement this biometric solution in all of its 256 outlets (Woszczyński, 2013, 2016). There were some other individual implementation projects in subsequent years, and the banking sector seems to have great expectations for biometrics in and broader range of applications (Figure 2).

Respondents pointed to areas which they thought would witness substantial implementations of biometric technologies in Poland by the end of 2020 (Figure 2). The coming years may prove to be a real biometric revolution in the Polish banking because experts anticipate an extremely wide range of applications for that technology in virtually every customer service channel. Almost all of the respondents are adamant that biometrics will function in bank outlets and in the ATM network. It seems substantiated due to the fact that this infrastructure is under direct control of the bank and

both of these service channels require the physical presence of the client. In the case of remote channels of communication with the bank, the respondents foresee the greatest role of biometrics (as many as 80% of the answers) in mobile banking, with only slightly fewer indications for telephone banking and mobile payments. The use of biometrics in online banking also recorded a very high share of the answers (58%). However, it should be noted that applying biometric solutions in that area is considerably impeded by the diversity of devices and software used by clients, and sometimes by the need to install a reader used in the authentication process. At the other end, the EFT-POS terminal network was named as the relatively most difficult area for the introduction of biometrics. This may be associated with a large number of geographically dispersed terminals on the one hand, and with consumer concerns as to the safety of using biometrics outside trusted infrastructure — belonging to their bank or in the form of the consumer's own device, on the other.

The opinion of the respondents is that the main biometric technology (Figure 3) to be applied when the client is physically present, i.e. in bank outlets, ATMs and EFT-POS terminals, will be the finger vein image. Fingerprints were also indicated in the case of terminals. When considering bank outlets, where technical capabilities may be used best, there were some additional answers indicating fingerprint biometrics, handwritten signature biometrics, scan of the iris/retina and hand biometrics.

In the case of mobile technologies, experts expressed the highest hopes for the use of fingerprints which may be introduced with relative ease on the client's smartphone (Figure 3). Voice biometrics was also rather popular — it may theoretically be used in each telephone device, but this solution may often pose problems with maintaining confidentiality. The finger vein scan received somewhat fewer indications, but it currently may not be implemented on a mass scale due to significant technical requirements for the mobile device. Surprisingly, face biometrics was unpopular among the experts, despite the fact that mobile devices are commonly equipped with cameras. Due to the vital role of the mobile channel in modern banking, it is analysed in more detail in the following chapter.

With reference to online banking, experts' opinions diverged strongly, making it impossible to indicate the leading biometric technology (Figure 3). It is worth noting that standard laptop components allow for the use of voice biometrics (28% — microphone) and face biometrics (19% — camera). In telephone banking based on Call Centres or Interactive Voice Response, the answer is unanimous, because the only option that may be used is voice biometrics (Figure 3).

Comparative analysis of authorisation methods in mobile banking

During the survey, the experts assessed individual transaction authorisation methods applied in mobile banking in Poland in terms of security and customer convenience (Figure 4). Respondents answered on a scale from 1 to 5, with 1 being the lowest mark and 5 the top mark. In terms of security, two authorisation methods decisively outscore other solutions: finger/hand biometrics and tokens. However, only one of them — biometrics — is at the same time highly convenient for consumers.

When considering convenience levels, two methods were judged as better than finger/hand biometrics: logging in to an application (without certification) and the PIN code. Yet, they provide a lower level of security, and in the case of merely logging in to an application it is so low that it practically disqualifies this method. Other solutions are also no match for finger or hand biometrics. One-time code cards, hardware tokens, and static passwords (especially masked) have an insufficient level of customer convenience. On the other hand, solutions such as: pattern and static passwords, and the aforementioned logging in to an application were marked by low security levels. Voice biometrics, SMS passwords, and mobile device certification[2] were assessed as average (Figure 4).

The presented results suggest that biometrics, in particular of the finger or the hand, seems to be a transaction authorisation technology with a strong outlook for success. This scenario is supported by the fact that in line with theoretical research models and the results of other studies provided in the discussion in earlier chapter, biometrics of this kind has two key characteristics boosting customer acceptance of the innovation: it simultaneously ensures a very high level of security and user convenience.

The abovementioned empirical results should be construed in the context of statistical data regarding the mobile devices market. According to Deloitte Global (2017), in mid-2016 30% of smartphones in developed countries had a fingerprint reader, and by the end of 2017 this share is to rise to 40%. A dynamically growing number of mobile devices can read this kind of biometric data, which also diminishes one of the barriers to the popularisation of biometrics in mobile banking related to technical limitations on the part of customers' devices (Saevanee *et al.*, 2015).

This makes it possible to apply selected biometric solutions in mobile banking on a mass scale. It is equally important that the owners of such devices have already largely accepted this solution for the purposes of daily

[2] A certificate is obtained for the hardware element of a mobile device in a procedure of authentication in another electronic channel, e.g. in online banking.

use of their telephone. As estimated by Deloitte, in the period of 2016–2017 the proportion of users actively using a fingerprint reader will increase from 69% to 80% (Deloitte, 2017). This makes a separate process of training consumers unnecessary. The solution should also be perceived by consumers as easy to use, which is one of the crucial factors in the adoption of a new technology.

Regulatory Technical Standards as a stimulus for the implementation of biometrics in the banking sector

In November 2015, the European Parliament adopted Payment Services Directive 2 ordering all member states to adapt national legislation accordingly by 13 January 2018 (European Parliament, 2015). One of the fundamental changes introduced by the PSD2 consists in providing stricter requirements for the security of payment transactions, such as obliging payment services providers to apply Strong Customer Authentication (SCA). This regards situations when the payer: (1) gains access to their payment account online, (2) initiates an electronic payment transaction, (3) carries out an action using a remote channel, which may involve a risk of payment fraud or other malpractice. The task of drafting the Regulatory Technical Standards concerning the requirements of strong customer authentication and secure communication was vested in the European Banking Authority. The standards are in the final preparation phase (European Banking Authority, 2017). According to the EBA, the proposed Regulatory Technical Standards on strong customer authentication and secure communication are key to achieving the objective of the PSD2 of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union.

In the case of Poland, in effect of the anticipated changes, the Polish Financial Supervision Authority introduced a recommendation (Komisja Nadzoru Finansowego, 2015) pursuant to which SCA requires banks to use at least two different authorisation elements, for instance, combining a method from the "something I know" group with a method from the "something I have" or "who I am" group. Moreover, it must be impossible to reuse or reproduce at least one of these elements (except for biometric identifiers). The prohibition concerning reuse may cause problems to the use of certified mobile devices (something I have) in connection exclusively with a PIN or a static password (something I know), which is currently a common solution in mobile banking. It seems that among the analysed methods (see Figure 4), the non-reproducibility and non-reusability re-

quirement is met only by one-time SMS passwords, tokens, and biometric methods. Of these three, finger/hand biometrics is by far the most convenient for users. Therefore, a combination of a certified telephone and biometrics seems more attractive than a set consisting in a certified telephone and an SMS password or token. In consequence, if the current shape of RTS is maintained, the legal regulations of the European Union will be a crucial driver of banks' interest in a wide use of biometrics for many years to come.

Conclusions

Due to being at risk of different kinds of attacks, the banking sector is deeply interested in ensuring high levels of security of the services it provides. Biometric technologies are one of the solutions it may apply. The results of empirical studies allow for assuming that the coming years will see truly revolutionary changes in the use of biometrics in Polish banking. Experts' forecasts indicate that by the year 2020 biometric technologies will be used in every customer service channel to a very broad extent. The experts are most optimistic with regard to the projected adoption of the biometric technology to the authorisation of customers in bank branches and ATM networks. The mobile channel, in turn, is perceived as the most important area for the expansion of biometric technologies among remote customer service channels. Dominant technologies will include: (a) finger vein biometrics — in the case of bank branches and ATMs; (b) voice biometrics — mainly in telephone banking; (c) fingerprint biometrics — in the case of mobile banking and mobile payments.

The authors' research indicates that authorisation with the use of the fingerprint is at the same time very secure and convenient for consumers in mobile banking. It is an extremely attractive solution as compared to traditional authorisation methods, and it can already be used on a mass scale. The chances for the implementation of that technology are high, due to the dynamically growing number of smartphones adjusted to reading fingerprints. A positive consequence of this phenomenon for the banking sector is that it will not have to build its own infrastructure for biometrics. The increasing number of devices equipped with fingerprint readers is popularising biometrics and customers do not have to be additionally educated because they use the technology willingly.

A further stimulus which should help materialise the biometric revolution in banking results from legal regulations in the European Union. It is expected that the implementation of Regulatory Technical Standards may

be a real catalyst for technological changes in the field of authorisation of banking transactions. RTS will make it necessary to replace such methods as PIN or password with more secure ones which, in turn, are mostly rather inconvenient according to research. As a result, biometric technologies will be the leading group of methods used, as they are marked by high levels of security and convenience of use. The course of this process will be an interesting field for future research.

Due to the fact that the work is focused on payment applications of biometric, it results in some limitations. It does not address ethical issues and privacy concerns, as well as consumers' view on the subject.

References

Aliyu, A., Younus, S. M., & Tasmin, R. (2012). An exploratory study on adoption of electronic banking: underlying consumer behaviour and critical success factors case of Nigeria. *Business and Management Review*, *2*(1).

Alterman, A. (2003), "A piece of yourself": ethical issues in biometric identification. *Ethics and Information Technology*, *5*(3). doi: 10.1023/B:ETIN.0000006 918.22060.1f.

Bank of England. (2015). Financial stability report. 37. Retrieved from http://www.snb.ch/en/iabout/pub/oecpub/id/pub_oecpub_stabrep (08.02.2017).

Bank of England. (2017). Financial stability report. 41. Retrieved from http://www.snb.ch/en/iabout/pub/oecpub/id/pub_oecpub_stabrep (08.02.2017).

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*. doi: 10.1016/S2212-5671(15)01077-1.

Bustard, J. (2015). The impact of EU privacy legislation on biometric system deployment: protecting citizens but constraining applications. *IEEE Signal Processing Magazine*, *32*(5). doi: 10.1109/MSP.2015.2426682.

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, *31*(5). doi: 10.1108/14684520710832315.

Deloitte (2017). *Technology media and telecommunications predictions 2017*. London. Retrieved from http://www.deloitte.com/view/en_RO/ro/industries /technology-media-telecommunications/513596b205d9d210VgnVCM2000001 b6f00aRCRD.htm (01.02.2017).

European Banking Authority (2017). Final report. Draft regulatory technical standards on strong customer authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) (Vol. 2366).

European Parliament. (2015). Directive 2015/2366 (Payment Service Directive 2). Official Journal of the European Union, L 337/35(260), 35–127.

Gaikwad, A. N., & Pasalkar, N. B. (2004). Biometric person identification—methods, advances and performance evaluation. *IETE Technical Review*, *21*(3). doi: 10.1080/02564602.2004.11417147.

HM Government (2015). 2015 Information Security Breaches Survey, 49. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf (02.02.2017).

Jagadiswary, D., & Saraswady, D. (2016). Biometric authentication using fused multimodal biometric. *Procedia Computer Science*, *85*. doi: 10.1016/j.procs.2016.05.187.

Khandelwal, C. S., Maheshewari, R., & Shinde, U. B. (2016). Review paper on applications of principal component analysis in multimodal biometrics system. *Procedia Computer Science*, *92*. doi: 10.1016/j.procs.2016.07.371.

Kim, C., Mirusmonov, M., & Lee, I. (2010). An empirical examination of factors influencing the intention to use mobile payment. *Computers in Human Behavior*, *26*(3). doi: 10.1016/j.chb.2009.10.01.3

Komisja Nadzoru Finansowego (2015). *Recommendation on the security of payment transactions carried out on the Internet by banks, national payment institutions, national electronic money institutions and cooperative savings and credit societies*. Warsaw: the Polish Financial Supervision Authority.

Koulayev, S., Rysman, M., Schuh, S., & Stavins, J. (2016). Explaining adoption and use of payment instruments by US consumers. *RAND Journal of Economics*, *47*(2). doi: 10.1111/1756-2171.12129.

Kubiszewska, K. (2017). Banking concentration in the Baltic and Western Balkan states – selected issues. *Oeconomia Copernicana*, *8*(1). doi: 10.24136/oc.v8i1.5.

Kumar, K., & Farik, M. (2016). A review of multimodal biometric authentication systems. *International Journal Of Scientific & Technology Research*, *5*(12).

Lancelot Miltgen, C., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "big 3" of technology acceptance with privacy context. *Decision Support Systems*, *56*(1). doi: 10.1016/j.dss.2013.05.010.

Lumini, A., & Nanni, L. (2017). Overview of the combination of biometric matchers. *Information Fusion*, *33*. doi: 10.1016/j.inffus.2016.05.003.

Malathi, R., & Jeberson Retna Raj, R. (2016). An integrated approach of physical biometric authentication system. *Procedia Computer Science*, 85(Cms). doi: http://doi.org/10.1016/j.procs.2016.05.271

Matyas, V., & Rilla, Z. (2002). Biometric authentication – security and usability. In *Advanced communications and multimedia security IFIP TC6TC11 sixth joint working conference on communications and multimedia security. September 26-27 2002 Portorož Slovenia*, 100(5). doi: 10.1007/978-0-387-35612-9_17.

Peng, J., El-Latif, A. A. A., Li, Q., & Niu, X. (2014). Multimodal biometric authentication based on score level fusion of finger biometrics. *Optik*, *125*(23). doi: 10.1016/j.ijleo.2014.07.027.

Pocovnicu, A. (2009). Biometric security for cell phones. *Informatica Economica*, *13*(1).

Polasik, M., Piotrowska, A., & Kumkowska, N. (2015). *Development through innovations or economies of scale? Study of the participants of the Polish payment system. Executive summary*. Retrieved from http://alterum.pl/uploaded/Raport_Rozwoj_przez_innowacje_czy_efekt_skali_-_polski_s.pdf (10.06.2017).

Polasik, M., & Wisniewski, T. P. (2009). Empirical analysis of internet banking adoption in Poland. *International Journal of Bank Marketing*, *27*(1). doi: 10.1108/02652320910928227.

Polasik, M., Wisniewski, T. P., & Lightfoot, G. (2012). Modelling customers' intentions to use contactless cards. *International Journal of Banking, Accounting and Finance*, *4*(3). doi: 10.1504/IJBAAF.2012.051590.

Saevanee, H., Clarke, N., Furnell, S., & Biscione, V. (2015). Continuous user authentication using multi-modal biometrics. *Computers & Security*, *53*. doi: 10.1016/j.cose.2015.06.001.

Sahoo, S., Choubisa, T., & Mahadeva Prasanna, S. (2012). Multimodal biometric person authentication: a review. *IETE Technical Review*, *29*(1). doi: 10.4103/0256-4602.93139.

Schierz, P. G., Schilke, O., & Wirtz, B. W. (2010). Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electronic Commerce Research and Applications*, *9*(3). doi: 10.1016/j.elerap.2009.07.005.

Seiders K., Voss G. B., Godfrey A. L., & Grewal D. (2007). SERVCON: development and validation of a multidimensional service convenience scale. *Journal of the Academy of Marketing Science*, *35*. doi: 10.1007/s11747-006-0001-5.

Shen, Y.-C., Huang, C.-Y., Chu, C.-H., & Hsu, C.-T. (2010). A benefit–cost perspective of the consumer adoption of the mobile banking system. *Behaviour & Information Technology*, *29*(5). doi: 10.1080/01449290903490658.

Shin, D.-H. (2009). Towards an understanding of the consumer acceptance of mobile wallet. *Computers in Human Behavior*, *25*(6). doi: 10.1016/j.chb.2009.06.001.

Szwajca, D. (2016). Corporate reputation and customer loyalty as the measures of competitive enterprise position – empirical analyses on the example of Polish banking sector. *Oeconomia Copernicana*, *7*(1). doi: 10.12775/OeC.2016.007.

Van der Ploeg, I. (2003). Biometrics and privacy a note on the politics of theorizing technology. *Information, Communication & Society*, *6*(1).

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, *27*(3). doi: 10.2307/30036540.

Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: a case study. *Information Management & Computer Security*, *16*(4). doi: 10.1108/09685220810908813.

Woszczyński, T. (Ed.). (2013). *Biometrics report* . Warsaw: The Polish Bank Association. Retrieved from https://zbp.pl/public/repozytorium/dla.../Raport_Biometryczny_2.0_strona_FTB.pdf (22.02.2017).

Woszczyński, T. (Ed.). (2016). *Report biometrics in banking – key aspects*. Warsaw: The Polish Bank Association. Retrieved from: https://www.bankbps.pl/__data/assets/pdf_file/0005/268646/Report_Biometrics-in-banking-key-aspects.pdf (22.02.2017).

Zhu, D. H., & Chang, Y. P. (2014). Investigating consumer attitude and intention toward free trials of technology-based services. *Computers in Human Behavior*, *30*. doi: 10.1016/j.chb.2013.09.008.

Annex

Table 1. Biometric technologies applied in banking

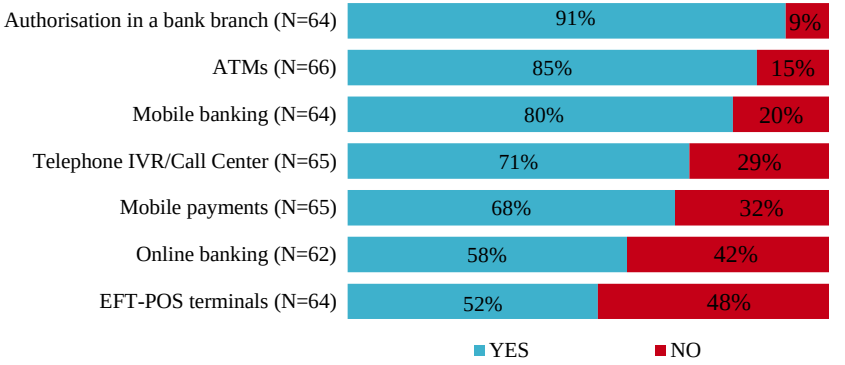
Biometric technology	Description	Security and convenience
Face recognition	The biometric system remembers identifiers located on the face of the identified person (the shape and positioning of the nose, eyes or ears).	Using cameras in ATMs and mobile devices benefits customer convenience. It may be somehow limited by the need to update the sample due to natural changes in face shape during the customer's life or changes resulting from events such as an accident or plastic surgery.
Fingerprint	The database stores an image of the fingerprint that may be additionally processed using advanced IT techniques.	The strength of this method lies in the assumption of the immutability and uniqueness of fingerprints. However, there is a risk related to the use of a copied fingerprint.
Hand geometry	The user is identified through hand shape, including the length and width of fingers.	A simple method, but may give rise to accusations of discrimination.
Iris/retina scanning	The biometric system remembers the iris or retina pattern individual for each human being.	A technology ensuring high security levels but at the price of high implementation costs and a limited level of acceptance on the part of the customers.
Voice print	The identification process is based on comparing the voice tone, timbre and strength with the sample.	The natural activity of speaking used in this technique facilitates its acceptance and makes this manner of collecting and verifying biometric data convenient for the customer. Drawbacks may consist in voice alterations in time or playing back recordings.
Signature recognition	The system analyses the shape of the letters and movement dynamics, among other factors.	If the system is too sensitive, it may fail to authenticate a transaction carried out by an eligible person. This is because there are no two identical signatures of the same person. Differences in handwriting may also result from changes in the emotional or physical state of the customer.
Finger vein	The finger vein scanner scans the finger using light close to infrared.	The arrangement of finger veins is not visible and thus cannot be copied. The scanning process lasts around a second, which is barely inconvenient for the customer.

Source: own work based on: Gaikwad & Pasalkar (2004), Peng *et al.* (2014) and Venkatraman & Delpachitra (2008).

Figure 1. Positions held by the respondents

Source: survey of representatives of institutions operating in the payment services market in Poland, N=70.

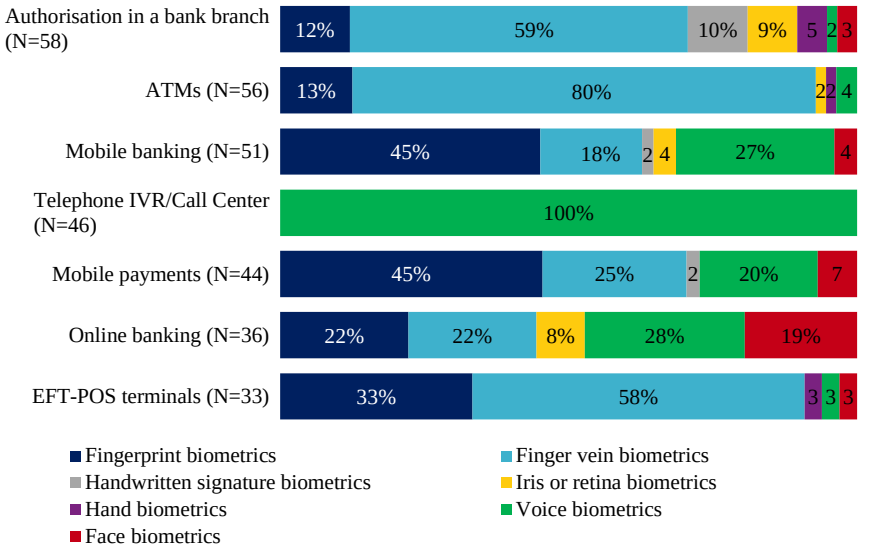
Figure 2. Expected implementations of biometric technologies in the Polish market by 2020



Q: What are the areas in which you anticipate new implementations of biometric technologies in the Polish payment services sector by the year 2020? If yes: in which technology?

Source: authors' own survey of the Polish banking sector.

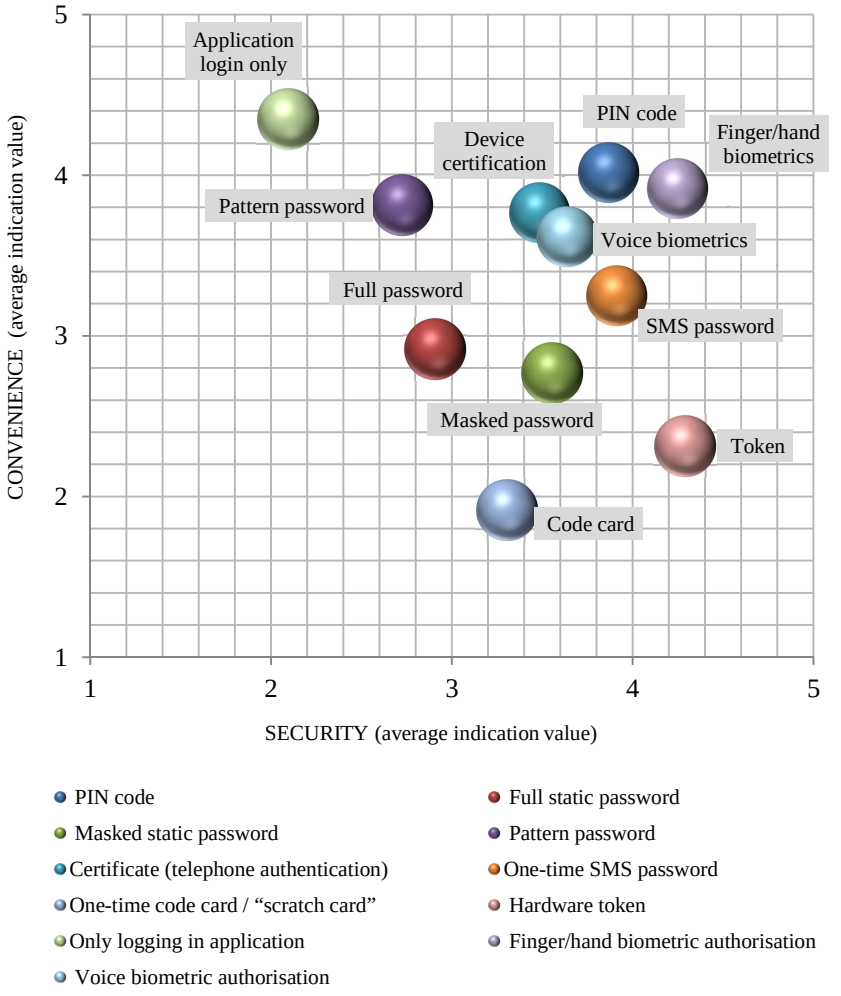
Figure 3. Technology in which biometrics will be implemented according to experts anticipating such implementation



Q: What are the areas in which you anticipate new implementations of biometric technologies in the Polish payment services sector by the year 2020? If yes: in which technology?

Source: authors' own survey of the Polish banking sector.

Figure 4. Transaction authorisation methods in mobile banking by security and customer convenience



Q: Assess individual transaction authorisation methods in mobile banking (in a scale of: strongly disagree – 1, disagree – 2; nether agree nor disagree – 3; agree – 4; and strongly agree – 5 in terms of security/convenience).

Source: authors' own survey of the Polish banking sector, Convenience: N=60 experts' responses; Security: N=66 experts' responses.