Guide for **Digital Payments**

MAY 2022

Centralna banka BOSNE I HERCEGOVINE
Централна банка БОСНЕ И ХЕРЦЕГОВИНЕ
WORLD BANK GROUP
Finance, Competitiveness & Innovation

TABLE OF CONTENT

1. INTRODUCTION **5**

2. THEMATIC SECTION – Types of Digital Payments and Consumer Rights Protection **7**

2.1. Various approaches to digital payments in BiH 7
2.2. What are mobile payment apps? 8
2.3. Activation and technical requirements for use of mobile payment apps 12
2.4. Mobile payment apps security features and abuse prevention 12
2.5. How do contactless payment cards and contactless bracelets work? 13
2.6. Requirements for use of contactless payment cards and bracelets 13
2.7. Contactless payment card/bracelet security features and abuse prevention 13
2.8. Basic obligations for digital payment service users 15
2.9. Fraudulent or deceptive practices users should be aware of 16
2.10. Consumer rights, complaint procedures and the institutions responsible for protection of consumer rights 20
2.11. Banking System Ombudspersons 22
2.12. Mediation as an option for out-of-court settlement 24

Questionnaire for readers to assess their knowledge 26
Glossary of Basic terms used in the Guide 28
Suggested useful links 30

Photo Credit: https://www.pexels.com/@pavel-danilyuk/

1. INTRODUCTION

With the development and technological progress of society, new financial user needs arise and new challenges are created in the financial market. One of the more recent developments is the emergence of new payment options for financial transactions. In addition to classic cash payments, various forms of digital, cash-free payments are now developed with the support of modern technologies. The COVID-19 pandemic has made digital payments even more practical compared to traditional payment methods, primarily due to lowering the likelihood of virus transmission. It is expected, given the further development of technology that these methods of payment and transfer of money will increase its share in total payments.

In this guide, we will focus on the latest trends in the digital, cash-free payments available to citizens in Bosnia and Herzegovina. Various cash-free payment options are becoming commonplace in the market and the dynamics and speed of development point to the need for more education and public awareness to ensure more responsible and safer use of cash-free payments.

Digital payments mean cash-free transactions, i.e., payments for goods and services which take place exclusively in a given electronic/ virtual environment.

The main feature of non-cash payments is that the transaction takes place without a physical transfer of money. This means that neither the payor (the person who pays) nor the payee (the recipient who receives the money) have any contact with cash. The advantage of digital payments is the fact that the payor can make payments anytime, anywhere, quickly and easily, using the selected technological solutions (for example, a special mobile app or entire service packages - mobile and/or Internet banking).

Digitalization of services requires educated users able use modern payment services in a safe and responsible manner. Educating consumers about their rights and courses of action in the event of misuse or fraud related to digital payments is equally important. In that regard, the latest market trends related to mobile and contactless payment options and their features will be discussed in more detail below, including various approaches to digital payments in BiH, main types of digital payments, technical requirements and users' obligations, as well as information about fraudulent or deceptive practices the users should be aware of. Also, this guide provides information about consumer rights and complaint procedures and includes a list of BiH institutions responsible for protection of consumer rights.

Photo Credit: https://www.freepik.com/rawpixel.com

2. THEMATIC SECTION – Types of Digital Payments and Consumer Rights Protection

2.1. Various approaches to digital payments in BiH

Different models, innovative approaches and services are available in Bosnia and Herzegovina digital payments available in. All banks in BiH issue payment cards (contact and contactless) for use on Pont-of-Service (POS) terminals and via the Internet (in physical and online environments). However, other options are increasingly present on the market. A basic distinction can be made between applications (apps) developed by commercial financial institutions such as banks and those that serve as a means to pay vendors for purchases or services provided. Overall, the goal is to make payments simpler, safer and faster while also taking into account the environmental benefits such as reduced use of paper and other resources. Apps pay special attention to payment and data storage security, so it is important be aware of the solutions the apps offer and whether these suit the user's needs.

For example, some companies offer a dedicated app for payment of their services that is linked to an account with a partner bank; the user downloads the app from popular services, registers (with card information, certain personal data and service reference number) and opens an account in the bank to keep the app active. The payment process is usually done in the form of recurring payment orders (notifications on payment due date) and there is no need to go to the bank or re-enter the details for each payment. It is common practice for a particular app to allow payments to multiple service providers. Financial institutions also provide their clients with various digital payment options, constantly updating their practices, helping to record transactions and facilitating their use (for example, additional security mechanisms that cover the payment process without having to confirm potentially risky transactions or data storage methods by special calls – tokenized approach, or the option to manage personal finance with cost accounting tools, etc.).

Check with your financial or other service provider for digital payment options. Ease or complexity of use, speed, additional payment options, lower cost for digital payments, whether the app is available only if you open an account with a certain bank or is perhaps linked to another type of service, etc. – those are the important questions to think about and seek answers to before making the decision to use digital payments.

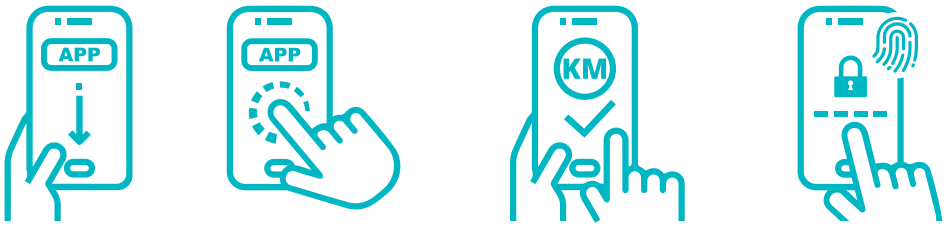
2.2. What are mobile payment apps?

Mobile payment applications (apps) are special software programs, developed for smartphones or tablets, which allow users to make different types of payments. In addition to payment features, these apps often have other features such as checking account balances, reviewing costs, submitting online applications, marketing and participation in promotional campaigns, communication with financial service providers and other consumer features.

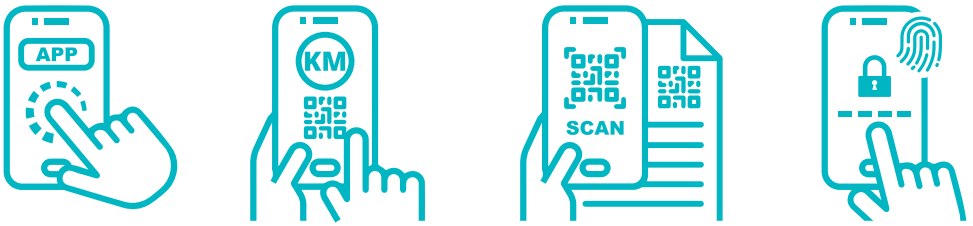
Various types of apps are available on the market and can be distinguished by the way payment services are provided. There are several payment options, and the most common ones are:

Art Credit: https://www.freepik.com/upklyak

i) Payments via electronic payment order are made by installing and launching the app and making the initial entry of the assigned PIN or biometric (usually a fingerprint). Payment apps already include software-defined elements of the payment order, which need to be filled in depending on the type of payment. This makes the use of the service easier. The most important elements of the order (selected and/or filled in by the user) are the selection of the account from which the payment should be made (only if you have multiple accounts), purpose of payment, recipient details (name and address), recipient's account details and the payment amount. Additional elements may be necessary only in the case of international payments or payment of public revenues. The completed order is confirmed by entering the PIN or biometrics again, when the payment is considered completed.



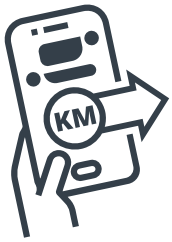
ii) Apps that can read Quick Response (QR) codes found on the invoices of vendors that offer this type of payment. After launching the app, select the payment option, scan the QR code on the invoice with a mobile device and authorize the payment with PIN or biometrics, after which the payment is considered completed.



iii) Payments using Near Field Communications (NFC) technology. You must activate this feature by enabling it in your existing mobile payment app (such as a mobile banking app) or by entering the required data, such as your payment card details, and activation of the NFC option in the mobile device settings. You make the payment by unlocking the mobile phone and putting the back of the mobile device to the contactless POS terminal, regardless of whether or not you have an internet connection. It is important to note that the app does not need to be launched, but in order to make a payment, it is usually necessary to enter the card PIN at the POS terminal. In this way, payment is possible without the payment card on hand.

Unlocking the mobile phone

Placing the mobile device on the contactless POS terminal



iv) Chat apps can also be customized and used as a payment feature. They are currently most often used to check the account balance, send money to people in your directory who have registered to receive money through the app and to pay some predefined types of bills (such as utilities, electricity, gas, etc.). Transaction amounts are limited (to 200 BAM, for example), activation is often linked to another existing digital service (such as mobile banking) and each payment is verified by entering the appropriate PIN.

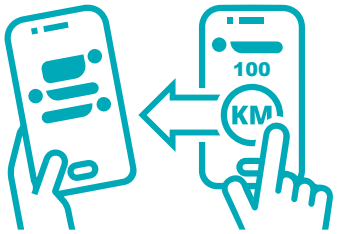


Photo Credit: https://unsplash.com/@jonasleupe

2.3. Activation and technical requirements for use of mobile payment apps

Payment is usually made by linking the app to your bank account or payment card. Activation of the app that is linked to your bank account usually requires a contractual relationship between the bank and the account holder and acceptance of the terms and conditions of use, either as a standalone service or as part of a particular service package. Such apps include mobile banking apps, chat banking apps and other specialized banking apps.

Activation of the app linked to a payment card usually involves online user registration, acceptance of terms and conditions and initial entry of card data necessary for making payments. In this case, the choice of apps is broader and includes various local and international apps available on online shopping platforms, which are not necessarily contractually connected to a particular bank.

Technical requirements include possession of a smart mobile device with an operating system that supports the mobile payment app you want to use. In this regard, it is necessary to be informed before choosing a service. In addition to the above, in most cases, it is necessary that the mobile device has a stable internet connection while using the application, and for chat banking also an active SIM card of the mobile operator.

2.4. Mobile payment apps security features and abuse prevention

Security is extremely important when paying and using mobile payment apps, so this means that all your data and access to the app are protected from abuse. User identification when opening the payment app and the authorization of payments are based on the PIN or passcode known only to the user or the user's biometrics (fingerprint).

For additional protection the screen of the mobile phone should be locked with another code known only to the user and different from the app PIN, and the user can also set biometric authentication for security purposes. If you are lending the mobile phone to someone to make a call or look up something, check beforehand whether you have logged out of all payment apps and apps that can access your accounts/money. Never leave your phone unattended.

When selecting the passcode or PIN, the user should avoid simple combinations of numbers (for example 1234, 1111, etc.), birthdays, wedding dates etc. Always be original and creative when choosing your passcode or PIN.

It is extremely important that you remember your PIN number and do not share it with anyone.

When selecting mobile payment apps, especially those that require online registration and entry of your personal data, such as payment card data, check whether the app is recognized on the market as verified and secure, how it uses your data and whether it has all the necessary security features. Download original apps exclusively from official online stores.

2.5. How do contactless payment cards and contactless bracelets work?

Contactless payment cards allow the cardholder to make payments at POS terminals by tapping the contactless POS device with the payment card. For amounts higher than BAM 60, the transaction must be approved by entering the card PIN. Contactless payment cards rely on the NFC technology and have a built-in electronic chip for secure and fast communication with the contactless POS terminal..

Contactless payment bracelets are based on the same principle as contactless payment cards, because they contain a mini card that must be tapped against a contactless POS terminals to effect the payment. Higher value transactions require approved by entering the PIN.

2.6. Requirements for use of contactless payment cards and bracelets

Contactless payment cards require a current account in a bank. The offer must be accepted by submitting a request and signing a contract, either independently or as part of a certain service package.

As a rule, the contactless bracelet is linked to your payment card and the corresponding account and is contractually provided as an additional mini card.

2.7. Contactless payment card/bracelet security features and abuse prevention

Contactless payment cards and bracelets should be kept safe and not given to others. This will protect the owner from potential abuse or unauthorized transactions. The PIN for authorization of amounts higher than BAM 60 must be remembered and not communicated to anyone.

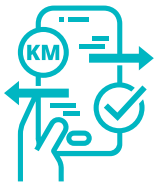
It is important to know that each transaction is secured by special encryption and that POS terminals do not allow duplicate payments for the same purchase, even if the card or bracelet is tapped several times.

Photo Credit: https://www.freepik.com/freepik

Photo Credit: https://unsplash.com/@proxyclick

2.8. Basic obligations for digital payment service users

The use of mobile payment apps and contactless payment cards and bracelets involves the acceptance of certain obligations by the user, primarily to protect themselves from potential misuse. In that respect, aside from safeguarding and not sharing one's codes (PIN), it is also necessary to keep in mind not to give our mobile devices, cards or bracelets to others. In case they are lost, the bank should be notified immediately to prevent any misuse.



Regularly checking one's account transactions is a must, so if you notice any transaction (however small, e.g. 2 BAM) that you did not approve or any other anomalies, report this to your bank immediately.

Checking transaction details. In fact, most app-based digital payment options enable double verification so that the user can be sure that they have entered the correct transaction data (recipient's given and family name, account number, amount, purpose, etc.).

Other obligations involve paying specific fees and commissions according to the pricing and the terms and conditions of the offer you accept each time you decide to use the services provided through a mobile app, card or bracelet.

If the available information about the service is not clear enough, or if you do not understand certain terms used in the description, you should seek clarification before using it.

If you are not certain a message or email you have received was sent by the service provider (information about the service, commercial offers, notice of a change in the service capacity, etc.), do not open that message or email. Especially if the message includes an invitation to submit your personal data. In such cases, you should verify the authenticity of the message and its purpose with the service provider.

It is good practice to always inquire about the offers and terms before selecting a service. If the offer is not sufficiently clear and transparent or acceptable in terms of cost, you should avoid using it in order to prevent unforeseen costs or other harm.

2.9. Fraudulent or deceptive practices users should be aware of

Technological advancement and new features made possible by mobile apps, contactless payment cards and bracelets also bring risks in terms of possible fraudulent or deceptive practices. It is important to note that legitimate and verified apps are continuously updated with the latest software solutions to offer the highest level of protection against data theft and fraud. However, even with these protections in place, it is important to be aware of potential frauds and the user's responsibilities when using a particular app or link and when sharing data. In this respect, the most frequent examples of fraud involve social engineering – when the user, through their own actions, makes the data theft or fraud possible. Some examples of phishing, vishing/voice phishing and smishing are described below.

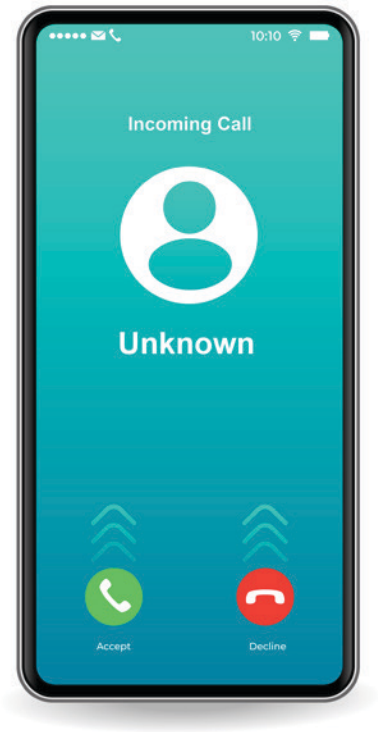
- **Phishing** involves various social engineering techniques used to steal data from users of financial services. The victim is often contacted through popular social networks with enticing offers or links. This type of fraud can emerge in the form of attractive or enticing titles, promises, seemingly credible content that is meant to entice the user to click and establish the connection. Most often these attempts involve vishing and smishing.

Art Credit: https://www.freepik.com/upklyak

- **Vishing,** or voice phishing, happens when a victim is contacted via telephone through false representation and is asked to provide their payment card, bank account or similar data.

An example of vishing

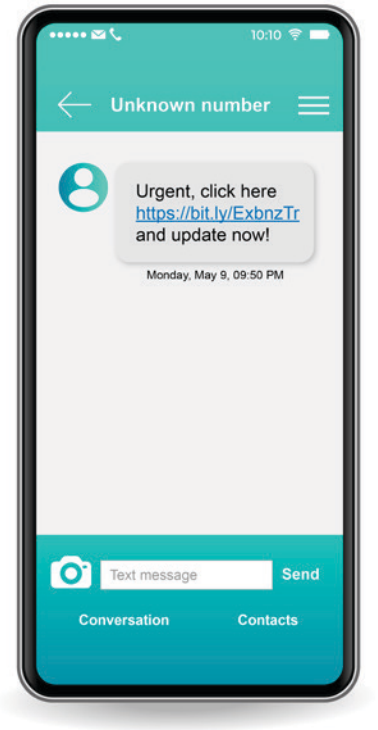
The victim uses a contactless payment card for daily purchases. One day they suddenly receive a call from an unfamiliar number and a person posing as a bank official with an urgent request to verify the card data in order to pay out a 100 KM award the victim won at the bank.



- **Smishing,** or textual phishing, happens when an SMS or a chat app message is sent from an unfamiliar number with enticing content urging the victim to click on a specific link. By opening the link, the recipient often unwittingly installs malware, i.e., a harmful app capable of stealing their personal data from the mobile device.

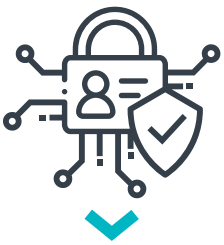
An example of smishing

A person who uses a mobile payment app suddenly receives an SMS from an unfamiliar number saying that, as of the next day, the installed payment app would no longer work on their mobile device and that they should immediately install a new one using a link attached to the SMS.



Aside from these examples, there are other fraudulent practices aimed at abusing the user's data in order to gain unauthorized access and conduct illicit transactions. Another frequent fraudulent practice is the shortened URL, a web address that is often (although not always) masking a malicious URL with the intent to commit fraud. That is why it is important to remain vigilant. You should be aware that shortened URLs are also frequently used for legitimate purposes, for example in the social media (although in such cases the full address is visible). But with malicious intent it is difficult for the user to see the full URL (hidden data) and clicking these links could lead the user to fake websites. Be mindful and visit only legitimate websites. Learn more about "secure options" for websites.

It is important to be vigilant and always adhere to basic security rules:



1. **Use antivirus software on your smartphone**
2. **Regularly update your apps**
3. **Only install apps from an official online store**
4. **Memorize and do not share your access data** (passwords, PIN, etc.)
5. **Consider using 2-step verification** (most of the leading platforms and apps now offer the 2-step verification option)
6. **Stay informed about tokenization options** (using a token for digital identification) **or securing your transactions with 2-step verification through SMS**
7. **Do not click on content from unverified or suspicious sources**
8. **Never share your card information**
9. **Cover the keyboard when entering your PIN into a POS terminal**
10. **Regularly check your bank statements and immediately report any unusual transactions to your bank**
11. **If using an app or another digital payment method involves accepting the terms and conditions, read them before accepting and seek clarification where necessary any unusual transactions to your bank**
12. **Never use devices with hacked and/or illegally unlocked** (rooted, JailBreaked, patched) **OS or devices which were used for access to illegal websites, such as torrent sharing sites, as these sites often contain malicious code which can infect your device and make it vulnerable to hacking and theft of personal information.**

If the user is using a payment application on a public network or is unsure of the network's security level for sharing personal data, consider using encryption or using a Virtual Private Network (VPN). If using VPN, the recommendation is to use a verified VPN which will usually be subscription-based.

2.10. Consumer rights, complaint procedures and the institutions responsible for protection of consumer rights

Digital payment options are often safe, but safety requires users to adopt responsible practices and behaviors. The level of security of digital payment services is proportional to the level of responsibility exhibited by the user. Fraud and deceptive practices still occur sometimes, even if the user is vigilant. Should this be the case, users should be aware of the consumer protection framework and how to use it.

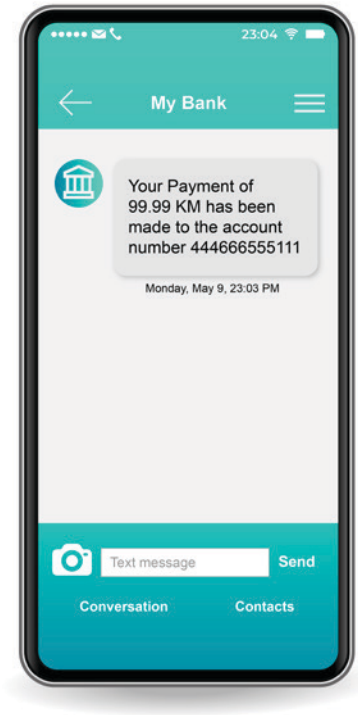
The key laws in the legal framework for consumer protection are the FBiH Law on the Protection of Users of Financial Services and the RS and FBiH Banking Laws. These laws specify the rights and obligations of consumers in all stages – from the initial stages of promoting and negotiating payment services to the final stage of a signed agreement between the financial service provider and the user. The law also outlines the rights and obligations of the financial institutions in terms of required level of information transparency and security. The laws stipulate the provisions that banking service agreements need to contain, including precise obligations and rights of the parties, service details, cost and duration of services, notices and contract amendments, contract termination procedure, protection of user rights and interests, etc. (for completeness the important provisions should be mentioned here - edit).

Before using any digital payment options (or any other financial product or service) it is advisable to read the general terms and conditions. Laws in BiH stipulate the obligations of financial institutions related to service transparency, meaning that each service should be clarified through the agreement, as well as other documents. You should read the contract and other documents. You have the right to seek clarifications of terms and provisions. Provisions relating to obligations of contractual parties are important to better understand which obligations belong to you, and which to the service provider.

Photo Credit: https://www.freepik.com/

Initial Detection of Misuse

The first and most important step is to immediately report any misuse or error to your bank (e.g. any transaction in your bank statement that had not been approved by you, loss of a payment card or bracelet, realization that you installed an app containing malware, etc.). It is important to monitor the state of your account(s), check and keep track of personal information.



The bank will take unilateral, necessary steps to protect your bank account depending on the type of report. In practice that may involve blocking your payment card or bracelet, blocking mobile or chat payments, double-checking how the transaction was made and whether an authorization or another action was necessary in the given situation.

What if access to the service is temporarily suspended?

In order to regain access to digital banking services or obtain a new payment card or bracelet, you must submit a written report/complaint to your bank. The written report should contain details of the transaction (e.g. date, name, amount of transaction, suspected misuse of data, etc.) and a request to return the funds to your account (if there were any charges or withdrawals from your account without your authorization) as a result of the reported abuse. The user should keep a record of communication with the bank.

In line with the laws and bylaws, the bank will review the user's contract, verify the circumstances of the report. The Bank will notify the user on the steps undertaken and report back on the submitted report/complaint

Immediately report abuse, suspicious transaction or loss of a card/bracelet to the bank.

The bank will take the necessary steps to protect your bank account

2.11. Banking System Ombudspersons

If the user is not satisfied with the bank's response or has not received a response within 30 days after the written report, the user can contact the Banking System Ombudsperson in the relevant entity banking agency. It is important to note that complaints to the Banking System Ombudsperson can be filed within six months from the date of receipt of the service provider's response or from the expiration of the prescribed 30-day period for the service provider's response. The procedure is free of charge.

Contact information for entity Banking System Ombudspersons:

Banking Agency of the Federation of BiH

Ombudsperson for the Banking System

Address: **Zmaja od Bosne 47b, 71000 Sarajevo**

E-mail: **ombudsmen@fba.ba**

Telephone: **033 569 787**

Banking Agency of Republika Srpska

Ombudsperson for the Banking System

Address: **Vase Pelagića 11a, 78000 Banja Luka**

E-mail: **info@abrs.ba**

Telephone: **051 224 079**

Upon receiving the complaint, and depending on each individual case, the Ombudsperson will review the complaint and decide whether it is justified. The Ombudsperson will inspect the actions of the bank and the user, analyze submitted documents showing the timeline of the discussions between the parties and review the grounds for the complaint. Depending on received information, the Ombudsperson decides whether to open a case or not. If the Ombudsperson decides not to open a case, they will advise the user to seek further action with other relevant institution. Depending on the situation, this may include re-communication with the financial service provider or a protection of rights through court proceedings. If the Ombudsperson opens a case, s/he conducts the complaint procedure and issues a recommendation to the bank. The Ombudsperson's decision is not legally binding.

It is important that the complaint contains the necessary and precise information of the transaction and the complaint should be accompanied by the relevant documentation.

A complaint must consist of:

1. **The user's name and surname**
2. **The user's postal address and contact telephone/email**
3. **The name and surname, address and contact telephone/email of the user's attorney** (in case a complaint is sent through an attorney)
4. **The business name and address of the bank**
5. **Detailed information about the dispute between the parties, when and where it happened**
6. **Any applicable attachments** (e.g., a copy of the previous complaint sent to the bank, a copy of the bank's response, a copy of the banking service agreement, other documents connected with the dispute such as power of attorney, etc.)
7. **Date and place of your complaint**
8. **Signature** (in case of sending a complaint letter)

The Ombudsperson's recommendations/opinions are not binding (unlike court decisions), but can be used as arguments and are important in further proceedings (either with a financial institution or a court), especially given that the Banking Ombudsperson operates within the Banking Agency as a regulator of the commercial financial market.

2.12. Mediation as an option for out-of-court settlement

Alternatively, if the parties agree, the recommendation may involve launching a mediation procedure with the Banking System Ombudsperson in order to seek a solution. In order to resolve issues and exercise their rights, parties may agree to launch a mediation procedure with the Banking System Ombudsperson and thus seek a solution.

Mediation is one of the options for out-of-court settlement. The advantage of the mediation procedure is that it is more flexible, simpler and cheaper than a court procedure. It is important to point out that the consent of both parties is necessary to initiate the procedure and that the procedure cannot be initiated unilaterally. During mediation, the mediator (the Ombudsperson) cannot impose solutions, but can facilitate communication and provide expert advice to help the parties find a solution.

- Mediation is a voluntary procedure which is not legally binding, but it is more flexible and cheaper than court proceedings
- The parties jointly submit a request to initiate mediation. It is not possible to submit a request unilaterally
- The request is submitted in writing
- The mediator does not impose solutions, but they can help facilitate communication and provide advice
- The mediation procedure itself is free of charge

If the Ombudsperson is not in charge of the given complaint, they can advise the user to seek further action with other relevant institutions and of the steps they should undertake.

Given that digital payments are often made to purchase goods and services, disputes and complaints are sometimes not related to the digital service provider but the retailer selling the goods or services. In such cases, general consumer protection rules apply. In Bosnia and Herzegovina, shopping, online shopping or distance shopping, is regulated by the laws on consumer protection and rests under the jurisdiction of the BiH Consumer Protection Ombudsperson. You can learn more about the Institution of the Ombudsperson for Consumer Protection in BiH at www.ozp.gov.ba. Complaints can be submitted directly or via the official website.

Rights can also be exercised through courts. The judicial system in BiH, depending on the nature of the claim or the violation of rights, provides protection in various procedures. It is useful, in case of seeking protection of rights trough courts, to consult and seek professional legal assistance.

Photo Credit: https://www.freepik.com/pressfoto

Questionnaire for readers to assess their knowledge

Please note that each question has only one correct answer

1 **What is the main characteristic of non-cash payments?**

a) The transaction takes place without a physical transfer of money

b) The transaction takes place with a credit card

c) The transaction takes place only for online purchases

2 **Things you cannot do with the mobile banking application?**

a) Check the account balance

b) Create a payment order

c) Sign a contract

3 **Contactless payment cards operate based on which technology?**

a) NFC

b) DFC

c) FNC

4 **For your safety, it is extremely important to:**

a) Remember your PIN number and share it with some close friends (for help in case you cannot remember)

b) Protect all your data, as well as access to the app, from abuse using PIN or passcode and biometrics

c) When selecting your passcode or PIN, use simple combinations of numbers to make the app easier to use

5 **What are the most frequent examples of fraudulent practices?**

a) Vishing

b) Calling

c) Chatting

6 **If you notice an unusual transaction, misuse, or error in the mobile payment application, the first thing you should do is:**

a) Regularly update your mobile payment application

b) Immediately report any misuse or error to your bank and provide the required information

c) Contact the transaction recipient and ask for clarification

7 **Which laws regulate the protection of users of financial services in the entities?**

a) Law on Financial Institutions in the Federation of BiH and Republika Srpska

b) Law on Protection of Users of Financial Services of the Federation of BiH and the Law on Banks of Republika Srpska

c) Law on Financial Consumer Protection in the Federation of BiH and Republika Srpska

8 **What is the role of the Ombudsperson for the Banking System?**

a) Protects the human and labor rights of the employees in financial institutions

b) Protects the rights and interest of banks

c) Protects the rights and interest of users of financial services and products

9 A financial service user can send a written complaint to the Banking System Ombudsperson in the relevant entity banking agency.

a) If the user is not satisfied with the service provider's response or has not received a response within 30 days from the written report

b) If the user does not trust the service provider and does not want any communication

c) If the user used an unregulated service to make the payment

10 The complaint to the Banking System Ombudsperson can be submitted within:

a) Twelve months from the date of receipt of the service provider's response

b) Nine months from the date of receipt of the service provider's response

c) Six months from the date of receipt of the service provider's response

11 What can the Banking System Ombudsperson offer as an option for out-of-court settlement of a dispute?

a) Mediation

b) Reconciliation

c) Representation before a court

12 Laws (on consumer protection for users of financial services/products) in BiH stipulate the financial institutions' obligations when it comes to:

a) Price range of digital payment services

b) Service transparency and the rights and obligations of consumers in all stages

c) Using 2-step verification in mobile payment apps

List of correct answers from the questionnaire

Question	Right answer	Question	Right answer
1	A	7	B
2	C	8	C
3	A	9	A
4	B	10	C
5	A	11	A
6	B	12	B

Glossary of Basic terms used in the Guide

ATM

Automated teller machine (ATM) is an electronic banking outlet that allows customers to complete basic transactions without the help of a branch representative or teller. Anyone with a credit card or debit card can access cash at most ATMs.

Bank account

A bank account is a financial service/product. It is an account maintained by a bank and used for payments and deposits. Each financial institution (bank) sets the terms and conditions for each type of account it offers.

Contactless payment

Contactless payment cards allow the holder of such card to make payments at POS terminals by tapping the contactless POS device with the payment card. Contactless payment bracelets are based on the same principle as contactless payment cards because they contain mini cards that need to be tapped against contactless POS terminals to make the payment.

Debit Card

Debit card is connected to a current bank account. The holder may dispose with the funds available on the account using the debit card.

Digital Financial Services

Financial services supported by modern technologies and offered via mobile phones, point-of-sale devices and over the Internet. Digital services can dramatically lower the costs for customers and service providers.

Protection of the rights of users of financial services

The rights of users of financial services are regulated by a number of laws and regulations adopted by regulatory institutions and represent the legal framework for protection of the users of financial products and services.

Financial Institution/Financial service provider

A financial institution is a company engaged in the business of offering financial services and products and dealing with financial and monetary transactions such as deposits, loans, payments, investments and currency exchange. In Bosnia and Herzegovina, the most common financial institutions on the market are banks, microcredit organizations and leasing companies.

Fraud

Fraud is a practice of deception through which a person is financially cheated by another person. There are many different types of fraud in finance or banking. Some of the most common types of fraud are debit and credit card fraud, phishing, digital payment fraud, safe deposit box fraud, etc.

Malware

Malware (short for "malicious software") is a file or code (delivered over a network) designed to disrupt, damage, steal or gain unauthorized access to a computer system.

Mediation

Mediation is one of the options for out-of-court settlement of disputes. The advantage of the mediation procedure is that it is more flexible, simpler and cheaper than a court procedure.

Mobile application

A mobile application or app is a software application or computer program designed to run on a mobile device such as a smartphone, tablet or smartwatch.

Mobile banking

Mobile banking uses mobile phones as a channel for provision of financial services. Mobile banking supports payment transactions such as money transfers, checking accounts and, in some cases, loan repayments, personal budgeting, etc.

Mobile payment

A mobile payment is a financial transaction performed through a mobile device or another portable electronic device. It is a financial product or service. Mobile payments are a financial service and/or product and can also be used to send money to others.

NFC (Near-Field Communication)

Near-field communication (NFC) is a set of communication protocols used for communication between two electronic devices over some distance (4 cm or less).

Banking System Ombudspersons in Bosnia and Herzegovina

The Ombudsperson for the Banking System is an institution established at the entity level to promote and protect the rights and interests of citizens as users of financial services. There are various rights protection mechanisms, such as complaint procedures and mediation.

Payment authorization

Payment authorization is a process that makes the payment more secure through verification. User authentication when opening the payment app and payment authorization are based on a PIN code or a passcode known only to the user, or the user's biometrics (fingerprint and/or retina scan).

Passcode

A passcode is a numeric sequence used to authenticate the user on computers and other electronic devices.

Phishing

Phishing is a fraudulent cyber-attack practice often used to steal user data, including login credentials and credit card numbers. The most common mode of attack is to trick the recipient into clicking a malicious link.

PIN

A personal identification number (PIN) is a numerical code used as an identification mechanism, mostly in electronic financial transactions. Personal identification numbers are usually linked to payment cards, mobile banking, various forms of digital payments and may be required to complete a transaction.

Point-of-sale (POS) device

A small, portable device that facilitates electronic financial transactions. POS devices can serve as banking outlets in certain cases. This device is used in trading and purchases when making cashless payments for various goods and services. Because they are inexpensive and easily transportable, they play an important role in closing the location gap and bringing access to financial services to rural areas and areas with underdeveloped infrastructure.

QR code

Quick Response or QR code is a two-dimensional version of the barcode, typically made up of black and white pixel patterns. Each QR code contains certain information (of different types) that the software can easily read. QR codes make the payment process easier, etc.

SMS (Short Message Service)

Short Message Service or SMS is a technology for sending short text messages between mobile phones. SMS is often used for verification (use of services, payments, etc.).

Vishing

Vishing is a fraudulent practice, a combination of 'voice' and 'phishing,'. It is a phone scam or voice message designed to get the user to share personal information.

VPN (Virtual Private Network)

A virtual private network, or VPN, is an encrypted connection to an Internet network. The main purpose of VPN is to establish a secure network connection when using public networks and helps to protect data transmission.

Suggested useful links

Useful links for institutions

Central Bank of Bosnia and Herzegovina: www.cbbh.ba
Central Bank of Bosnia and Herzegovina - financial education website: fined.cbbh.ba

Banking Agency of the Federation of BiH / Ombudsmen for the Banking System:
www.fba.ba; www.fba.ba/bs/ombudsmen-18
www.fba.ba/objection-form/1760
E-mail: ombudsman@fba.ba

Banking Agency of Republika Srpska / Ombudsmen for the Banking System:
www.abrs.ba; www.abrs.ba/en/ombdsman/c90;
E-mail: info@abrs.ba

Follow Us:

www.cbbh.ba
Twitter: @CBBiH
YouTube channel: Central Bank of Bosnia and Herzegovina
Facebook: www.facebook.com/CentralnaBankaBiH
LinkedIn: www.linkedin.com/company/cbbih

Central Bank of Bosnia and Herzegovina
Public Relations Service
pr@cbbh.ba
contact@cbbh.ba
+387 (33) 278 123
+387 (33) 201 517

The World Bank
E-mail: bih@worldbank.org
Phone: +387 (33) 251 500
Web: www.worldbank.org/en/country/bosniaandherzegovina
Facebook: @WorldBankBiH


Art Credit: https://www.freepik.com/freepik

Centralna banka
BOSNE I HERCEGOVINE

Централна банка
БОСНЕ И ХЕРЦЕГОВИНЕ

WORLD BANK GROUP
Finance, Competitiveness & Innovation