ANDROID STATIC ANALYSIS REPORT

FirstPay (6.0.1)

File Name:	FirstPay.apk
Package Name:	com.fmfb.firstwallet
Scan Date:	Jan. 4, 2025, 8:55 p.m.
App Security Score:	**51/100 (MEDIUM RISK)**
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	27	1	2	1

FILE INFORMATION

File Name: FirstPay.apk
Size: 52.63MB
MD5: ebac435ca82d8b32471da0fabc6a3560
SHA1: c473b591754e10bb64e513de3079b05319dfe6a4
SHA256: 6407a1064f5c08b640d4d8636acfd80ac5223f783372ae9289177effa4095351

APP INFORMATION

App Name: FirstPay
Package Name: com.fmfb.firstwallet
Main Activity: com.fmfb.firstpay.ui.authNew.activities.SplashNewActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 6.0.1
Android Version Code: 89

APP COMPONENTS

Activities: 23

Services: 19

Receivers: 26

Providers: 7

Exported Activities: 9

Exported Services: 2

Exported Receivers: 14

Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-04-25 12:12:00+00:00
Valid To: 2049-04-25 12:12:00+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x4cf306142a142c79625dc28b084c049e1c53551c
Hash Algorithm: sha256
md5: 5cec655bcdd75efb3c884ab4ceebef9f
sha1: 13250327509738f208fb374e31dc611137adb788
sha256: 089ce43c13c1427edfbf0b6a3d162e7a62fef653f5b86355da8762346dd64f27
sha512: 2e6cd64b5c1ba8478566ea41b770ae7f78483e00d68dae184091acc291209c545ccde30f54fed5dfc77706e68c70eb5ea3c7a9e778ae8a9d641687fc1083e1a4
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: de8618e244e2e47795d8d0aa473a4c0e509ed30e2266845db0e8398ab30e0bb7
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.apps.photos.permission.GOOGLE_PHOTOS	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.STORAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
com.fmfb.firstwallet.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.fmfb.firstwallet.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dexlib 2.x</td></tr></table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.fmfb.firstwallet,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **26** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Activity (com.fmfb.firstpay.ui.barcode.ScanActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.fmfb.firstpay.ui.authNew.activities.AuthActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.fmfb.firstpay.ui.auth.activities.OnboardingActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.theartofdev.edmodo.cropper.CropImageActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Activity (com.fmfb.firstpay.ui.home.activities.HomeActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (com.fmfb.firstpay.common.sms.receiver.SmsBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.onesignal.GcmBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Broadcast Receiver (com.onesignal.BootUpReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Broadcast Receiver (com.onesignal.UpgradeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Broadcast Receiver (com.onesignal.GcmBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Broadcast Receiver (com.onesignal.BootUpReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Broadcast Receiver (com.onesignal.UpgradeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
15	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
16	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
17	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityHMS) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
18	Broadcast Receiver (com.onesignal.notifications.receivers.NotificationDismissReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
19	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
20	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
23	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
24	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
25	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
26	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
27	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
28	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://firstwalletandroid.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/629046517181/namespaces/firebase:fetch?key=AIzaSyDZcAaUJStGYBZGd7cAGnrltJXdCQXYDBw. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.INTERNET, android.permission.READ_PHONE_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.READ_CONTACTS, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	5/44	android.permission.CALL_PHONE, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

❗ OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.hblmfb.com	ok	**IP:** 172.67.42.155 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firstwalletandroid.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

✉ EMAILS

EMAIL	FILE
example@gmail.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "4e9ef3645f5dfbc61f9031b6063b881f"
"faceoff_key" : "MTcwLDE1OCwxOTAsMTA2LDUyLDE2MCwxNDUsNzEsODgsOSwxNjAsMjQxLDY1LDU0LDIyNCwyMjUsNTEsOTYsMjQ1LDIyNSwxOTEsMTI5LDI0NCwxMTIsNDksMTUwLDE1OSwxMiwyMTgsMjI1LDc4LDIyOCwyNDgsMTY1LDI3LDEsMjE2LDE4NywxNTUsODksMjA3LDEyNSwxNDksMjksMTcsMjEyLDcwLDE5Miw3MCwyMywyMDIsMTkxLDM5LDE4NSwyMDIsMTQzLDE4Nyw4MywyNDksMTI0LDUxLDIxNywxNTIsNTcsMjE0LDI1MCwyMTQsMjM4LDIwNywxODEsNiw5MCwxMjAsMjM4LDg3LDIwMiwyMzgsMTUyLDIzNiwyMjAsMTE2LDE3MSwxNzQsMjUxLDIzMywyMTQsMTIxLDEwMiw2OCwxNjAsMjI4LDU4LDIyNCwxMjcsMTQ4LDE4OSwyMiwxNTYsMTM4LDEwMSwyOCwxNiw0MSwxOCwxNzEsNzcsMTEwLDE2OCwxODksMzMsMjEsMjcsMjQyLDE5NCw2NiwxNjcsMTI0LDYzLDE4LDY0LDE2MywxNzMsMTIzLDE2NSwxMjQsMjUyLDI1NSwyMTYsMjA5LDE1NCwzOCw5Niw2MCw5NiwxNTIsMjA2LDIxNCw5NCwxODQsMjE4LDE2MSwxMTAsMjEzLDE5MywxMDEsMTc1LDEzOCw5MCwyMjMsMjIwLDE4OSwyMzUsMjQyLDc0LDg4LDUwLDE5MCwyMDYsMTM1LDI1LDc2LDg0LDIyNiwxODEsMjM5LDE1OSwyNDcsMzIsODIsMCw2MiwyMDgsMTE4LDIxNCw2MCw3Miw2Niw5OSwxNDQsMTY0LDEzOCwyNDMsMTk3LDMyLDIwNSw1NiwyNiwyNDEsMTk2LDg5LDE2LDcyLDU4LDEyMiwxLDEwMyw0MCwyMjUsMTc3LDI0MSwxOTAsNTYsMjQxLDI2LDUsMTY5LDQxLDIxMSwyMTAsMjQ5LDk3LDI1LDIxNiwxNzQsMSwyNDIsMTc2LDExOCwyMjUsMjMxLDMxLDY3LDU1LDIzOSwzNiwxNTUsMTMzLDE4MywxMTEsMTI4LDc2LDM1LDE0Nyw1NSwyNTIsMTcyLDIyNywxNSwxNjYsMTQsMTM4LDE5NCwxMTAsMzksMTU5LDEyMCwxMTIsMTg4LDg0LDE1NywyMzYsODUsODQsOTYsMTk0LDI0OSwxLDAsMSw="
"firebase_database_url" : "https://firstwalletandroid.firebaseio.com"
"google_api_key" : "AIzaSyDZcAaUJStGYBZGd7cAGnrltJXdCQXYDBw"
"google_crash_reporting_api_key" : "AIzaSyDZcAaUJStGYBZGd7cAGnrltJXdCQXYDBw"
"maps_api_key" : "AIzaSyCAdQhyyneOnxvfsKuR0w1L4cQ98By9QZM"
ec0f1f44-3468-4d8f-bb5e-df80bca8bd0d

PLAYSTORE INFORMATION

Title: FirstPay

Score: 3.860465 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.fmfb.firstwallet

Developer Details: HBL Microfinance Bank Ltd, HBL+Microfinance+Bank+Ltd, 16th &17 Floor, HBL Tower, Blue Area, Jinnah Avenue, Islamabad, https://fmfb.pk, muhammad.yasir@hblmfb.com,

Release Date: May 5, 2019 **Privacy Policy:** Privacy link

Description:

What's New Account Linking & De-linking: Link your HBL Microfinance banking account to your FirstPay wallet and enjoy using a wider range of features across your HBL Microfinance account and the FirstPay Wallet. Favorites: Easily save your most frequent transactions and recipients as favorites for quick access, making repeat payments and transfers faster and more convenient. Cashpoint Visibility: View nearby HBL Microfinance Bank branches, ATMs, and authorized agents to help you locate cashpoints and banking services effortlessly. FirstPay by HBL MicroFinance Bank Ltd. About FirstPay: FirstPay, a mobile wallet powered by HBL Microfinance Bank is here to give you real Banking beyond the Branch experience. With a single tap, now send and receive money, linking of HBL Mfb account, access a loan with flexible payment plans, pay utility bills, and get mobile top-ups done for any network, from anywhere, anytime! So why wait? Sign up for FirstPay today and bring the bank home! FirstPay Features: • Instant Funds Transfer – Send and receive money to: o FirstPay wallet o Bank Accounts like Alfalah, UBL, Faysal Bank, or any other bank across Pakistan o Mobile wallets like EasyPaisa, JazzCash, Zindigi, SadaPay, or NayaPay • Mobile Load – Prepaid & Postpaid mobile load on any network • Mobile Bundle – Telenor • Utility Bill Payments o Electricity o Gas o Water o Internet o PTCL and many other bills • Instant money with Nano Loan o Apply for a Nano loan without any hassle of document submission and get up to Rs. 15,000 loans in no time! • Account Linking/De-Linking o Now conveniently link your HBL MfB account within the FirstPay app and enjoy the below features; o Fund Transfer from Core Bank Account o Utility Bill Payment o Account Balance and Transaction History o Cheque Book request and Status check o Stop Payment of cheque o Managing Bank Account Limits o Account Maintenance and Tax Certificate o HBL MfB Debit Card o Manage Dynamic QR o My Profits o My Loans and much more… • Debit Card o Forget the hassle of standing in long queues just for cash withdrawals. Order your FirstPay Debit card and enjoy a world of discounts at a wide variety of brands across Pakistan. • Debit Card Management o Manage your FirstPay Debit card - Debit card activation o PIN Generation o Temporary blocking & PIN Change o Statement of Account – get your account statement in just a click. o Dispute transaction - simply mark the transaction disputed through your statement and get it resolved • Invite Friends for more fun! o Now invite your friends and family to FirstPay. • Request Money o When you need funds, request from your friends and family through FirstPay conveniently • Favorites o Now mark any beneficiaries as Favorite and make effortless Mobile Top Ups and money transfers to your favorite contacts. • What's more on FirstPay? o Education Fee – Pay school, college or university fees through FirstPay instantly o Pay your taxes, License Fees, Traffic Challans, Credit Card Bills, and many other payments with ease. Follow us on social media to know what's happening on FirstPay and download the FirstPay app today! We are super excited to see you on the other side. In case of any suggestions or complaints, please write to us at complaints@hblmfb.com, or call 24/7 at 0800-42563. Follow us at: • Facebook o https://web.facebook.com/FirstPaybyHBLMFB • Twitter o https://twitter.com/FirstPayHBLMFB • Instagram o https://www.instagram.com/firstpaybyhblmfb/

SCAN LOGS

Timestamp	Event	Error
2025-01-04 20:55:17	Generating Hashes	OK
2025-01-04 20:55:18	Extracting APK	OK
2025-01-04 20:55:18	Unzipping	OK
2025-01-04 20:55:19	Parsing APK with androguard	OK
2025-01-04 20:55:20	Extracting APK features using aapt/aapt2	OK
2025-01-04 20:55:20	Getting Hardcoded Certificates/Keystores	OK
2025-01-04 20:55:27	Parsing AndroidManifest.xml	OK
2025-01-04 20:55:27	Extracting Manifest Data	OK
2025-01-04 20:55:27	Manifest Analysis Started	OK
2025-01-04 20:55:27	Performing Static Analysis on: FirstPay (com.fmfb.firstwallet)	OK

2025-01-04 20:55:27	Fetching Details from Play Store: com.fmfb.firstwallet	OK
2025-01-04 20:55:27	Checking for Malware Permissions	OK
2025-01-04 20:55:27	Fetching icon path	OK
2025-01-04 20:55:27	Library Binary Analysis Started	OK
2025-01-04 20:55:28	Reading Code Signing Certificate	OK
2025-01-04 20:55:29	Running APKiD 2.1.5	OK
2025-01-04 20:55:33	Detecting Trackers	OK
2025-01-04 20:55:34	Decompiling APK to Java with JADX	OK
2025-01-04 20:55:48	Converting DEX to Smali	OK
2025-01-04 20:55:48	Code Analysis Started on - java_source	OK
2025-01-04 20:55:49	Android SBOM Analysis Completed	OK

2025-01-04 20:56:04	Android SAST Completed	OK
2025-01-04 20:56:04	Android API Analysis Started	OK
2025-01-04 20:56:10	Android API Analysis Completed	OK
2025-01-04 20:56:11	Android Permission Mapping Started	OK
2025-01-04 20:57:01	Android Permission Mapping Completed	OK
2025-01-04 20:57:02	Android Behaviour Analysis Started	OK
2025-01-04 20:57:08	Android Behaviour Analysis Completed	OK
2025-01-04 20:57:08	Extracting Emails and URLs from Source Code	OK
2025-01-04 20:57:24	Email and URL Extraction Completed	OK
2025-01-04 20:57:24	Extracting String data from APK	OK
2025-01-04 20:57:25	Extracting String data from Code	OK

2025-01-04 20:57:25	Extracting String values and entropies from Code	OK
2025-01-04 20:57:31	Performing Malware check on extracted domains	OK
2025-01-04 20:57:32	Saving to Database	OK

Report Generated by - MobSF v4.2.9

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.