# Redefining Digital Banking: ANZ's Pioneering Expansion into Multi-Wallet Ecosystems

Sridhar Lanka
Data Architect, EMIDS, USA

## Abstract

Online banking transformed financial services by putting emphasis on convenience, speed, and security. With contactless and smartphone technologies gaining widespread popularity, mobile wallets are now a necessity for customers to make payments across channels. ANZ has been at the forefront of integrating different mobile wallet technologies onto one platform, with the view to offering consumers more choice and access. This multi-wallet ecosystem approach enables numerous digital wallets such as Android Pay, Apple Pay, Google Wallet, Samsung Pay, Fitbit Pay, PayPal and Garmin Pay, with cross-platform support and frictionless payment integration. The ecosystem also encompasses robust security features such as biometric authentication and real-time digital card updating. ANZ provides efficient transaction processing, fraud detection, and analysis across all wallet platforms through real-time data architecture and robust API connections. This strategy is a component of a wider banking ecosystem idea, wherein ANZ collaborates with partners to serve evolving client demands while safeguarding data and regulatory compliance. This strategy helps ANZ gain from the rise in demand for digital payments, develops more resilient client relationships, and drives financial services innovation.

**Keywords:** Digital Wallets, Android Pay, Fitbit Pay, Garmin Pay, Fraud Detection, API, Data Security, Regulatory Compliance

**DOI:** 10.21590/ijtmh.2024100105

## Introduction

Electronic payments, or digital payments, are payments in lieu of a service or product made with electronic means or devices like computers, phones, or payment cards. The methods render transactions more convenient, efficient, and traceable without the need for cash. Digital payments can be made with online banking, prepaid cards, debit cards, credit cards, payment apps, mobile wallets, peer-to-peer fund transfers, QR codes, contactless payments, and cryptocurrencies. The primary players in an electronic payment transaction are the payee (consumer), the payer (merchant), the issuer (payer's financial institution), and the acquirer (merchant's financial institution). Secure technology and payment networks enable efficiency and security. Electronic payments have transformed everyday financial transactions and business, delivering advantages in terms of higher ease, security, transparency, and financial inclusion, particularly for underprivileged groups. Their development shows continuous innovation by way of technology and changing customer requirements [1].

Mobile banking has come to evolve as a core revolution in the domain of digital financial technology with convenience, ease, and accessibility. Adoption, however, is not equal, and therefore researchers have looked to determine the determinants that affect user acceptability. Demographic factors, including age, gender, income, education, employment status, and marital status, are crucial in influencing individuals' perception and intention toward mobile banking services. Moderating the effect of behavioral constructs of perceived convenience, trust, and ease of use on usage are a combination of variables. This study draws a lesson from history by calling for empirical research into the extent to which demographic factors shape mobile banking adoption. The study seeks to offer actionable recommendations to financial institutions on how to modify their offerings in line with the distinct needs and preferences of particular demographic groups. The outcomes are predicted to inform adoption levels driving tactics and customer satisfaction within the fast-changing online banking setting [1].

Financial technology has transformed the conventional bank, mobile banking being a defining feature that provides efficiency, convenience, and accessibility. Adoption rates are not consistent and are moderated significantly by demographic variables. Ease of use, trust, and convenience are moderated by heterogeneous factors. Companies like ANZ are positively reacting to digital transformation with the creation of mobile wallets and facilitating secure, ongoing digital payments between different devices. This process involved cross-functional working across product, data, marketing, security, and technology functions. The bank made it possible for easy synchronization of digital credentials, instant transaction authentication, and robust, scalable fraud protection by combining mobile wallet functionality with ANZ's core banking platform [2].

A study that empirically analyzes the demographic factors that influence the usage of mobile banking service is to be performed by making recommendations to banks to adopt custom-made mobile banking services according to the needs and preferences of different population segments, based on the analysis of data coming from various users. Innovative initiatives such as ANZ's Mobile Wallet Transactions Expansion symbolize how the study can inform strategies for boosting levels of adoption and enhancing the general usage experience within the fast-evolving digital banking arena.

Mobile wallet capabilities have significantly boosted customer trust and adoption levels, with banks such as ANZ incorporating them into their consumer banking systems. It has led to an easy, secure, and timely payment transaction, enhancing consumer confidence while making online payments. Benefits such as protection from fraud, real-time transaction verification, and synchronisation of digital credentials in a secure way instil consumers' faith in their financial information. Integration with mobile wallets also simplifies transactions by eliminating the need to use physical cards or cash, enabling customers to make payments rapidly and safely in one touch. With this ease of use come increased rates of transaction success and improved acceptance, with some companies noting high usage levels. Mobile wallets enable automatic tracking and redemption of incentives, thus encouraging repeat usage and interaction. Customer satisfaction and adoption levels are highly correlated with service quality, usability, security, and ease of use. In summary, mobile wallet functionalities promote user confidence and uptake through the profitability, security, and convenience of digital payments [3].

The use of mobile wallet increases confidence in digital payments through ease of use and security. Sophisticated security features such as tokenisation, encryption, and biometric authentication restrain the access of payment details by third parties or nullify attempts at fraud. These actions address issues of fraud and data breach. Mobile wallets also enable synchronous payment credential synchronisation and real-time transaction verification, making the payment system efficient and trustworthy. This minimises the element of human error and enhances user trust in e-payments. Research indicates that more than 80% of individuals globally believe that their wallet data in the mobile is safe, greater trust than the wider population has in companies' data security. This facilitates regular and more reliable web payments because of transparent safety processes and convenience of one secure platform for multiple transactions [4].

Biometric authentication is a safe and unique method of verifying identity for mobile wallets, minimizing fraud risk and unauthorized access. Biometric features such as fingerprints, faces, or voices are hard to fake or fake, unlike passwords or PINs. Due to this simple and fast process of authentication, users can verify payments by finger touch or eye glance, establishing trust in the mobile payment system. This frictionless experience reduces transaction friction and puts an end to the necessity of tedious passwords. The combination of additional security and convenience brings increased confidence and trust, which boosts trust in the digital payments ecosystem. Mobile wallet faster checkout options reduce friction and uncertainty while paying, making consumers less apprehensive. Such features as instant payment buttons, autofill, and biometric authentication make payments easier, reducing known issues such as password memorization or waiting in line. Functions also increase the sense of security by a guarantee that information is secure and by eliminating the fear of fraud or loss of data.

Therefore, customers are likely to make payments using mobile wallets because of the convenience and security of faster checkout options [5].

## Methodology

This research investigates the moderating effect of demographic variables on mobile banking adoption through a quantitative approach. A stratified random sampling technique was employed to facilitate representation within significant demographic groups. The market target is customers who have utilized mobile banking services, specifically individuals who have used mobile wallet systems, such as those provided by ANZ's Mobile Wallet Transactions Expansion program. An online survey was administered to bank customers to collect information on population characteristics, opinions on mobile banking, mobile wallet and mobile banking utilization in real life, and experience with biometric login and rewards program integration. The theoretical framework consists of perceived convenience, perceived utility, trust, security, and ease of use as independent variables, and mobile banking adoption based on usage intensity and frequency as the dependent variable.

The study employs data from ANZ's Mobile Wallet Transactions Expansion initiative to place the empirical results into context, analyzing the impact of greater security functionality, cross-functional collaboration, and the embedding of mobile wallet capabilities within core banking systems on users' confidence and take-up rates. Participants were assured confidentiality and anonymity, and taking the survey was completely voluntary. The methodological method employed by ANZ in creating, implementing, and sustaining the data and technical infrastructure for the rollout of mobile wallets.

1. **Data Architecture Design and Integration:**
    - Real-time event-driven data architecture for wallet transactions across all platforms.
    - Facilitates high-volume transaction handling through fast data ingestion and processing.
    - Maintains precise identity management, fraud prevention, and efficient transaction reconciliation.
2. **Integration of Platforms:**
    - Data interface development between ANZ's internal banking platforms and digital wallet services.
    - Third-party integration for protected data sharing and compliance with regulations.
    - Protected data pipelines to safeguard PII and enable safe mobile wallet connections.
    - Cybersecurity and Compliance to impose secure access controls and multi-factor authentication solutions.
3. **Dashboards and Real-Time Analytics:**
    - Development of custom dashboards and analytics solutions to monitor transaction volumes, user patterns, wallet adoption rates, and fraud information.
    - Delivery of actionable insights for data-driven decision-making in order to enhance campaign effectiveness and client interaction.
4. **Compliance and Security:**
    - Ensuring top priority to data security and compliance with APRA and PCI-DSS standards.
    - Adoption of encryption, masking, and anonymisation techniques to sensitive information.
5. **Leadership in Teams:**
    - Management of cross-functional teams by security architects, BI analysts, and data engineers.
    - Strategic Advisory Role by translating business objectives into technological data solutions.

The High-Level Architecture Overview describes an event-driven, real-time data architecture for analytics, security, compliance, and multi-platform mobile wallet integration, as detailed in your methodology. Mobile Wallet Integration Layer Key Elements are illustrated in Figure 1:

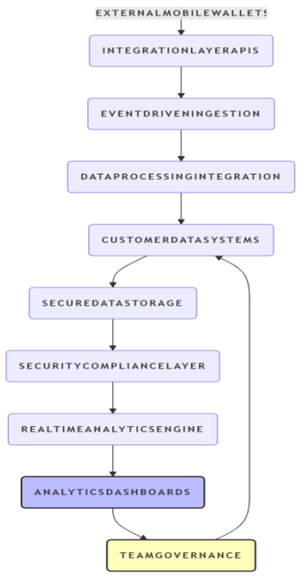


**Figure 1:** Mobile Wallet Transaction Platform Architecture

Mobile Wallet Integration Layer is an essential part of the banking system, offering secure APIs for transaction initiation and authentication to enable support of different device ecosystems. The layer captures real-time wallet transactions as events through message brokers such as Kafka and AWS Kinesis so that all the transaction data is available immediately for processing. It integrates with core banking systems for fraud detection, account management, and client data for fraud protection, transaction reconciliation, and effortless identification verification.

The Transaction Data Store maintains transaction events with the safety and up-to-dateness of the client profiles and authentication data. Analytics Data Marts are optimized for reporting adoption trends, user activity, and transaction volumes. Payment data and personally identifiable information are secured through data encryption and tokenisation at the Security & Compliance Layer. Audit trails and access controls impose multi-factor authentication, role-based access, and comprehensive logging. Regulatory compliance is assured by APRA, PCI-DSS, and other standards. Real-Time Analytics Engine offers real-time insights through streaming data processing, whereas interactive dashboards and reporting tools enable interactive fraud data tracking, user activity, and transaction volumes. Product and marketing teams are offered practical guidance based on data. The diagram shows the flow of data between modules within a system by visually linking them and showing various functions or subsystems.

It starts with external wallets, flows through the integration layer, gets ingested and processed, stored securely, and checked for security and compliance. The diagram also represents dependencies and interactions among modules, showing which modules communicate with one another. The diagram also represents how data is modified or enriched as it progresses through each phase, with each module having a unique role to play. Despite being a block diagram, not an official data flow diagram (DFD), it is at a high enough level that it is simple to understand the logical movement of data and the important points of contact. It can be applied to certain kinds of interactions or types of data, but it gets across the general flow and module interconnection points well enough to most audiences. The diagram also describes how modules communicate with data stores, how module communication points define foreign objects, and how it depicts data transformations and process orderings [6].

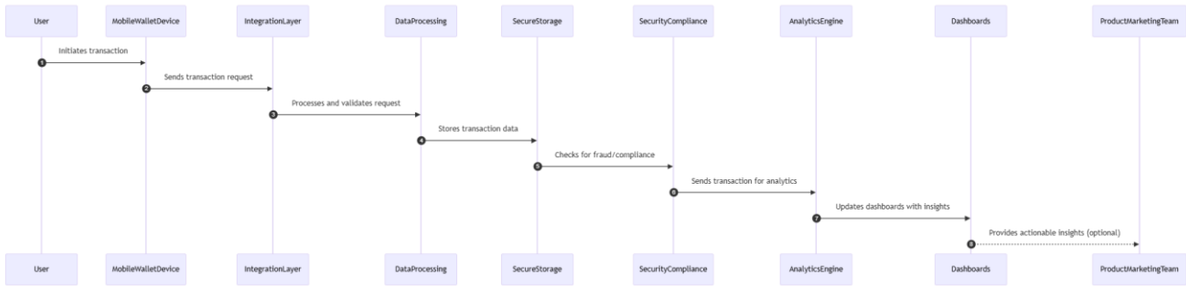


**Figure 2:** Sequence Diagram for Mobile Wallet Transaction Platform

This sequence diagram (Figure 2) shows the flow of the mobile wallet transaction, from user choice to data processing and validation. The transaction starts when the user chooses a payment mode in the application on their phone. Thereafter, it goes through several stages such as processing, security checks, dashboard refreshes, analytics, and ultimate verification. The API gateway accepts the transaction request from the device, and the business logic is applied by the data processing module. The data gets secured storage in a database or data store for future use and reconciliation. The security and compliance module gets notifications from the secure storage, does real-time fraud detection, and checks for compliance with legal mandates. The transaction is routed to the analytics engine for real-time analysis of consumer behavior, fraud detection, and usage trends. The analytics engine refreshes dashboards and reporting tools with the most recent transaction data, offering key insights to product and marketing teams. The diagram also exhibits critical characteristics like clear sequence, modularity, security and compliance, real-time analytics, and cross-functional collaboration. This diagram correctly illustrates the typical process of a secure, scalable, and analytics-based mobile wallet transaction platform, as per industry best practices.

ANZ has demonstrated notable multi-wallet growth by employing a mixed-methods strategy, integrating both qualitative and quantitative research approaches to guide its digital innovation. Technical challenges, cross-functional collaboration, strategic goals, and learning were discussed with key stakeholders such as product managers, security architects, marketing personnel, and tech leaders in semi-structured interviews. Document analysis was also used to learn about architectural design, security practices, and governance models. Customer usage information was gathered from ANZ mobile payment systems, such as Android Pay, Apple Pay, Google Wallet, Samsung Pay, Fitbit Pay, PayPal and Garmin Pay. Customer opinions were obtained through surveys regarding the simplicity, security, trust, and satisfaction of making payments using multiple wallets. Technical analysis of compliance processes, data security controls, event-driven architecture in real-time, and API integration allowed for multi-wallet support. Statistical techniques such as regression analysis and descriptive statistics identified variables that influence consumer adoption as well as consumption habits in different wallet systems. Triangulation, anonymizing customer information, and participant consent for surveys and interviews validated the study. But the research might not apply to other marketplaces or banks because it is based on ANZ's experience and confidentiality agreements that bar access to essential corporate information and proprietary technological details [7].

ANZ's multi-wallet strategy is supported by a Digital Ecosystem Framework, integrating different systems such as Google Wallet and Apple Pay into a single ecosystem. Critical metrics are cross-platform and device compatibility, API interoperability with external vendors, and scalability of pipelines for real-time information. Security-Compliance Matrix has data encryption, tokenisation, audit trails, and fraud analytics. The Real-Time Analytics Architecture Model leverages event-based data flows to enable real-time insights for monitoring. The Cross-Functional Governance Model targets API integrations for data engineering, security and compliance rule adherence, and marketing campaigns for customer adoption and engagement. The Regulatory-Strategic

Alignment Framework features multi-regulator coordination and industry standards such as interoperability with the New Payments Platform (NPP) [8].

Customer-Centric Adoption Model puts user control, trust, and convenience at the forefront. The ANZ Technical Blueprint Implementation Insights initiative confirms event-driven architecture with DLT for settlements involving multiple currencies. The Ecosystem Strategy entails breaking down platform silos leveraging Finastra's "connected banking" principles. These models entail technological implementation, customer adoption, regulatory compliance, and strategic governance, which are all central to measuring multi-wallet ecosystems. Coordinating these elements was paramount to ANZ's success, evidenced by their real-time fraud analytics and cross-device functionality presented in Figure 3 [8].

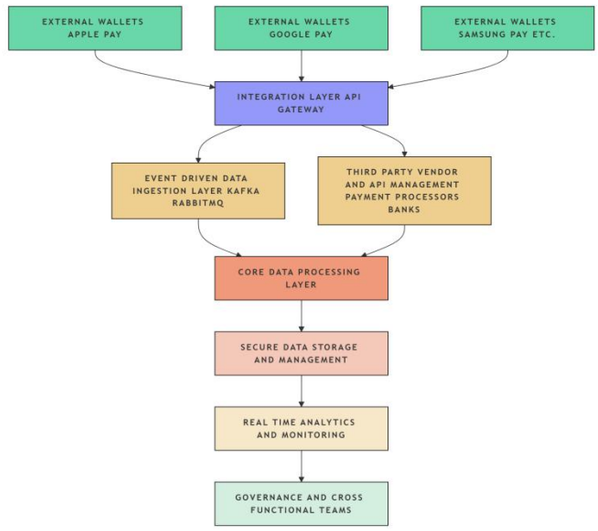


**Figure 3:** Real-Time Fraud Analytics and Cross-Device Functionality

ANZ Mobile Wallet is a contactless payment platform enabling customers to make secure payments via smartphones and wearables. It accommodates various platforms and employs an event-driven, real-time architecture to capture wallet transactions, enabling identification verification, fraud detection, and transaction reconciliation. It also synchronizes data among ANZ internal banking systems and digital wallet services, securing data integrity and compliance with the law. Secure data pipelines are architected using encryption and tokenisation in order to protect personally identifiable information (PII) and enable secure wallet connections. Cross-functional cooperation with cybersecurity, risk, and compliance departments mandates multi-factor authentication, audit trails, and secure access controls. Dashboards and real-time analytics are developed and deployed to monitor fraud data, wallet adoption trends, transaction volumes, and user behavior in real time.

Compliance and security are maintained by anonymizing, masking, and encrypting sensitive data. The ANZ Mobile Wallet is backed by a multi-disciplinary team of security architects, BI analysts, and data engineers, and acts as a strategic adviser to the senior leadership. In July 2017, ANZ was the only major Australian bank to offer four mobile payment systems to both iOS and Android smartphones. In December 2017, ANZ added support for customers with compatible Garmin devices. The ANZ Mobile Wallet is rated as one of the most technologically advanced banking apps in the Asia-Pacific region by Forrester and IDC.

## Challenges

Before 2017, ANZ had a number of challenges in promoting digital payment solutions. Some of the challenges include low adoption of digital payments with customers experiencing security concerns, fragmented support on platforms, and limited device support. The ecosystem was also fragmented, with banks supporting only one or two prominent mobile wallet platforms, creating a discontinuous user experience. Customers needed to wait for replacement cards if their cards were stolen or lost, which disrupted them from performing transactions. ANZ

also did not have real-time visibility of transaction volumes, customer engagement levels, and usage trends of mobile wallets on different platforms. This disrupted fraud detection, personalizing engagement methods, and enhancing the customer experience. To curb these challenges, ANZ introduced a holistic digital payment program featuring multi-platform mobile wallet integration, a digital card continuity feature, and a real-time data framework [9].

The bank now offers support for the major mobile wallet platforms, providing cross-platform accessibility for consumers to make payments online with the device of their choice. The digital card continuity feature enables consumers to replace their digital wallet information in the event of loss or theft of the physical card, enhancing convenience and security. The bank's data-driven approach enabled it to make objective decisions and strengthen its digital payment services over time [6]. Before 2017, mobile payments were significantly curtailed by restricted device compatibility, impacting owners of widely used products such as Samsung, Garmin, and Fitbit. The majority of banks had limited support for a few mobile wallet platforms, including Apple Pay or Android Pay. Un-supported devices from the selected bank's platform were excluded from mobile payments. Not all banks were part of each mobile payment system, even for supported devices. This incompatibility was a setback for the full adoption of mobile wallets, and customer satisfaction and ease were diminished. Regardless of the limitations, most customers could not fully access the convenience and security benefits offered by mobile wallets [10].

Historically, mainstream mobile wallets have been only available in a limited number of systems, like Apple Pay or Google Wallet, backed by a large number of banks and payment card processors. Customers with non-participating devices, like Samsung phones or wearables like Fitbit or Garmin, couldn't add their cards to the wallet or make payments using it. Older or less mainstream hardware or operating systems usually did not support security features or application compatibility, and so users of specialized or legacy devices were locked out from the ecosystem. The absence of mass-market support resulted in a dispersed user experience, with some users making mobile payments while others did it by cash or on traditional cards. Furthermore, older or unsupported devices would not get the latest software updates or security patches and hence would be less appropriate for secure financial transactions [11]. The digital platform of ANZ Plus features 875,000 active users, out of which an estimated 30,000 are added each month.

Mobile wallet payments in Australia have grown by 8,200% as a result of extensive usage, with 1.2 million customers enrolling in Voice ID. Transaction value and revenue have also grown, with institutional payments up more than 60%. Payments and Currency Processing delivered $410 million in FY23, up by 23%. ANZ Plus says it achieves much lower operational and efficiency scores than legacy systems. System performance is measured by Google DORA metrics. ANZ's Security Operations Centre prevents more than $100 million in fraudulent transactions each year and blocks more than 10 billion threats. Customer protection features involve blocking scam SMS, removing phishing websites, and tracking attacks [12]. From table 1 it is indicated that various wallet platforms are being used more by ANZ consumers with transaction volume and share showing increased usage. Mobile wallets are driving considerable money flow, as indicated by total transaction value. Digital engagement KPIs demonstrates high consumer engagement with ANZ's digital channels. This table can be utilized in reports or presentations to emphasize ANZ's multi-wallet ecosystem reach.

**Table 1:** Key Product Impact Indicators ANZ’s Multi-Wallet Ecosystem

| Metric Category | Metric Description | Value / Data Point |
|---|---|---|
| Customer Adoption & Usage | Card Registrations | Nearly 700,000 ANZ debit and credit cards registered by Dec 2017 across Apple Pay, Android Pay, Samsung Pay, Fitbit Pay, Garmin Pay |

| | | |
|---|---|---|
| | Transaction Volume (Dec 2017) | ~3.9 million mobile wallet transactions (140% increase vs Dec 2016) |
| | Transaction Share (Dec 2017) | Mobile wallet transactions = 4.5% of all ANZ card transactions (up from 2% in 2016) |
| | Cumulative Transactions (May 2016 - Dec 2017) | Over 30 million mobile wallet transactions |
| Revenue & Financial Impact | Cumulative Transaction Value (by Dec 2017) | Exceeded $1 billion USD |
| | Digital Engagement | 3.4 million digitally active customers, 19+ million logins per week |

Customer satisfaction and experience are achieved through end-to-end service delivery, financial wellbeing tool usage, and regulatory compliancy with regulatory needs. Service principles are evaluated to guarantee consumer-focused ecosystem performance, emphasizing service, strategy, safety, and simplicity. Compliance Adherence ensures secure and reliable digital payments, and Service Principles guarantees consumer-focused ecosystem performance [13].

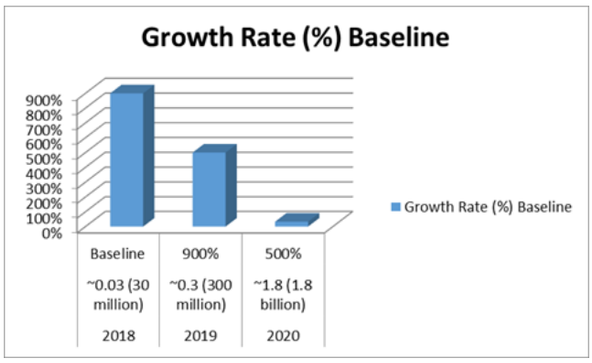


**Figure 4:** Mobile Wallet Transaction Growth Over Time

## Conclusion & Future Scope

ANZ has taken big leaps in Australia and New Zealand's digital banking domain by unifying multiple mobile wallet technologies into one, event-driven real-time architecture. This move has enhanced user simplicity, volumes, and security. ANZ Plus, with its more than a million users and likely to outshine every other retail banking platform by 2029, reflects the seriousness of ANZ towards digital transformation. The emphasis on safety and customer handling in the world where digital payments are becoming more prevalent is visible with the release of web banking without a password and the Digital Padlock option.

Future objectives for ANZ are full passwordless authentication by mid-2025, real-time customer control via the Digital Padlock feature, platform extension and unification by 2029, next-generation AI and analytics integration, open banking and ecosystem collaboration, sustainability and regulatory adherence, and reducing phishing and data breach-related risks, enhancing operational flexibility, and offering personalized financial services. ANZ's investment in these projects has made it a leader in safe, scalable, and customer-centric digital banking. The bank aims to transition all retail customers, including those acquired via Suncorp Bank, onto the ANZ Plus platform within 2029.

## References

1. "The moderating effect of demographic variables on mobile banking adoption: An empirical investigation", Deepak Chawla, Himanshu Joshi, Global Business Review, 19(3S) 1–24 © 2018 IMI, SAGE Publications.
2. "The Key Drivers Behind Consumer Mobile Wallet Adoption During Covid-19", Paul, April 9, 2022 https://passkit.com/blog/mobile-wallet-adoption/.
3. "How perceived trust mediates merchant's intention to use a mobile wallet technology", Nidhi Singh, Neena Sinha, Volume 52, January 2020, https://doi.org/10.1016/j.jretconser.2019.101894.
4. "Mobile Wallet Integration: A Wellspring of Opportunities and Challenges", Mehul Rajput July 30, 2019, PaymentsJournal, https://www.paymentsjournal.com/mobile-wallet-integration-a-wellspring-of-opportunities-and-challenges/.
5. "Are Biometrics the Answer to Mobile Payments?", Proof, August 3, 2022 https://www.proof.com/blog/are-biometrics-the-answer-to-mobile-payments.
6. "Data Flow Diagram with Examples & Tips", Larry Constantine, https://www.modernanalyst.com/Resources/Articles/tabid/115/ID/2015/Data-Flow-Diagram-with-Examples-Tips.aspx.
7. Transforming Diagnostics Manufacturing at Cepheid: Migration from Paper-Based Processes to Digital Manufacturing using Opcenter MES. (2022). International Journal of Research and Applied Innovations, 5(1), 9451-9456. https://doi.org/10.15662/IJRAI.2022.0501005
8. "The (not too distant) Future of Money is Digital", Nigel Dobson, Hari Janakiraman & Inga Bambalaite-Saliba https://www.anz.com/institutional/insights/articles/2022-04/not-too-distant-future-of-money-is-digital/.
9. "Mobile Payment and Digital Wallet Financial Services", The Department of the Treasury, Payments system review: From system to ecosystem, June 2021.
10. "Mobile payment systems fail to become the dominant payment method", moneytips.com (KSDK), August 11, 2017 https://www.ksdk.com/article/money/personal-finance/mobile-payment-systems-fail-to-become-the-dominant-payment-method/63-463616678.
11. "Payment Revolution: How Apple and Android Are Changing How We Pay for Products Today", Nick Babich, 11-20-2017 [Adobe Blog].
12. "Understanding Your Digital Wallet - and Six Ways to Keep it Safe", Cyber Security, Digital wallet, David Herbison, SVP, Director of Digital Banking Strategy, https://www.bannerbank.com/financial-resources/blog/understanding-digital-wallets.
13. "Evaluating ANZ's Financial Performance (2019–2023): A Secondary Data-Based Analysis Using Key Financial Ratios and Trend Analysis", DOI: 10.48175/IJARSCT-26639, ISSN: 2581-9429.
14. "Mobile wallet spending surges over holiday period", Steve Price Head of Everyday Banking and Payments, ANZ 19 January 2018 https://www.anz.com.au/bluenotes/2018/01/Mobile-wallet-spending-surges-over-holiday-period/.