Publication date:
June 2021
Author:
Helen Allingham

Mobile App Protection in Banking

Don’t let mobile security fall through the cracks

In partnership with:

Brought to you by Informa Tech

Contents

Summary

Overview

Mobile banking continued its spectacular growth trajectory in 2020, with financial services institutions (FSIs) worldwide, reporting a notable uplift in mobile banking users and digital engagement. Having already considered the fastest growing channel pre-COVID, the pandemic has accelerated the shift to mobile further still. Yet, while mobile technology brings numerous opportunities to FSIs, it also brings new challenges. Chief among these challenges is security. Mobile apps offer an entry point to an FSI's wider systems and as apps proliferate, so too do the number of entry points. However, with mobile app development typically sitting separately to core enterprise technology within FSIs, the protection of mobile apps can get lost between enterprise security teams and development, thus putting FSIs at risk of hacking and data breaches. This scenario is particularly concerning given the regulatory backdrop of data privacy and financial services regulations, which require FSIs to ensure personal data is fully protected.

To understand what steps FSIs can take to improve their approach to mobile app protection, analyst house, Omdia, and mobile application security specialist, Verimatrix, have partnered to produce this white paper on mobile app protection for financial services. Drawing on Omdia's ICT Enterprise Insights 2020/21 survey, the white paper looks at the rise of mobile financial services, the challenges of app protection, data protection regulations, and the technological approaches FSIs can employ to ensure their code is protected and their algorithms are secure.

Key messages

- Mobile is an intrinsic part of the financial services ecosystem. Among retail banks, mobile banking ranks as the top overall investment priority across all business functions in retail banking for 2021.
- From a technology perspective, managing security, identity, and privacy ranks as the highest priority for investment among FSIs. However, mobile app protection can often get lost between organizational cracks.
- A growing number of data privacy regulations worldwide require organizations to have the necessary infrastructure and processes in place to protect customer data or else risk large fines.
- Mobile app protection need not be a lengthy or overly onerous exercise. Employing automated security tools can enable apps to self-defend against external risks and provide an effective approach to app shielding.

Mobile app protection in financial services

Mobile has become an intrinsic part of the financial services ecosystem

The shift to mobile has been one of the definitive financial services trends of the last decade. Once an on-trend adjunct to online services, today mobile is increasingly the channel of choice for customer interaction.

In banking, fintech disruptors around the world have challenged the status quo with the launch of mobile-first banks that offer a slick, contemporary approach to banking more in keeping with today's digital lifestyle. Notable new providers include Nubank in Latin America, Monzo in the UK, and Chime in the US, yet there are many others.

Traditional banks, for the most part, are actively seeking to grow their mobile user base. Many institutions have sought to nudge customers toward digital banking options, as part of their efforts to reduce costly branch operations. Some institutions have also created their own separate digital banks to encourage development free of legacy constraints; small businesses bank Mettle launched by the UK's NatWest is a case in point.

2020 witnessed strong growth in mobile banking adoption

The COVID-19 pandemic has only served to accelerate this shift to mobile, pushing laggard customers to adopt digital banking services and pressing home the need for banks to invest in their digital capabilities and, in particular, mobile. Unsurprisingly, numerous FSIs worldwide reported significant growth in mobile banking users over 2020. Chase Manhattan, which has the largest active mobile banking user base in the US, reported 10% growth in mobile banking users, taking its total users to 40.9 million. A number of challenger banks have also reported particularly strong growth over the last year. Germany's N26, for example, announced it had reached 7 million customers in early 2021, up 2 million on the previous year.

The trend has not been confined to consumer banking, with providers also reporting increased uptake of mobile apps in business and corporate banking. Global player HSBC, for instance, announced a 146% increase of app downloads of its core business digital platform HSBCNet.

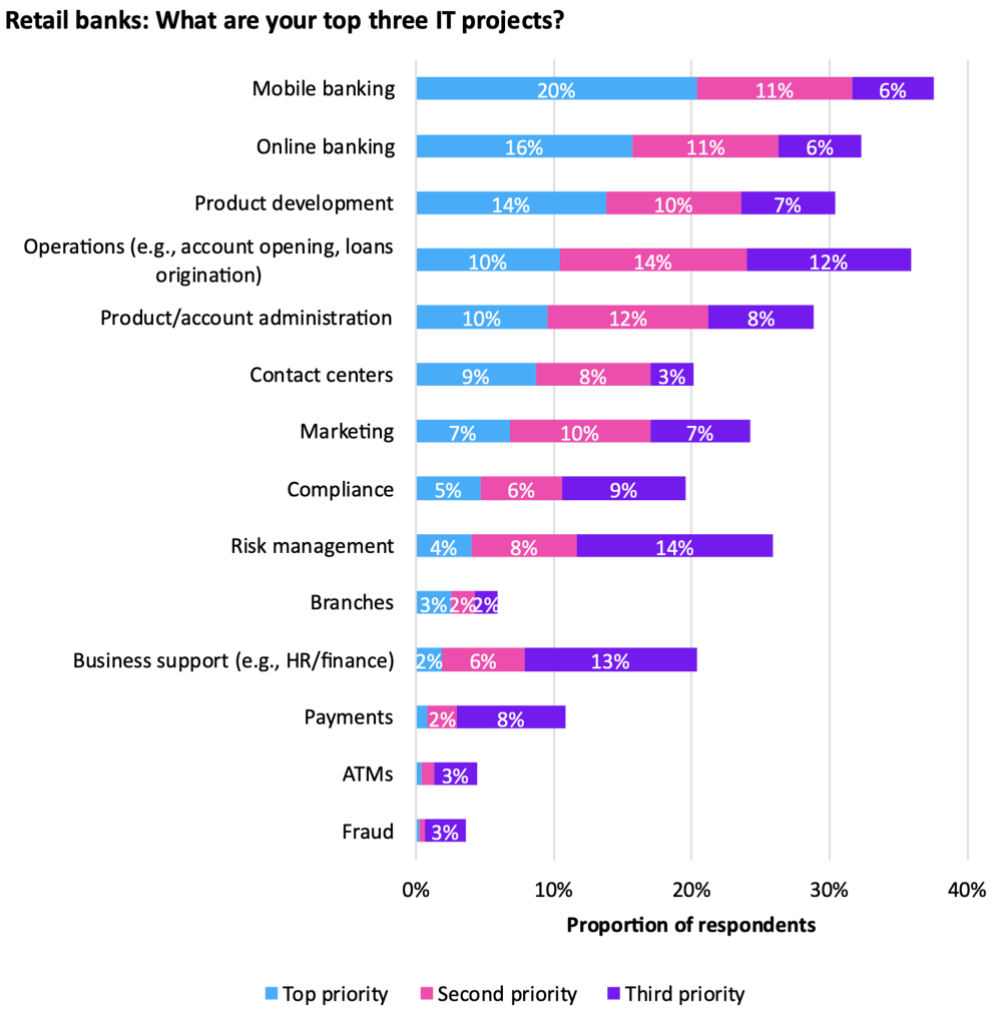
Improving mobile service offerings is a key priority for FSIs

Given this context, it is no surprise that developing and improving mobile service offerings is a key priority for financial services providers. FSIs are continually adding to their suite of mobile offerings, looking to add functionality to existing apps and launching new ones. In 2020, Spain's Santander announced a complete redesign of its mobile banking capabilities to include new capabilities such as

analysis of savings and spending patterns, while Monzo in the UK launched an account offering for small businesses. The rollout of 5G will also fuel mobile banking development, providing greater bandwidth to add new capabilities. Undoubtedly, the number and variety of mobile banking apps offered by FSIs will continue to proliferate in the coming years.

The findings of Omdia's ICT Enterprise Insights primary interview program with senior executives across 60 countries provide a clear reflection of this trend, with mobile banking cited as the highest-priority IT project among retail banks. Indeed, 37% of respondents placed mobile banking as a top three priority, while 20% placed mobile banking as their top priority IT project over and above other areas such as online banking, product development, and contact centers.

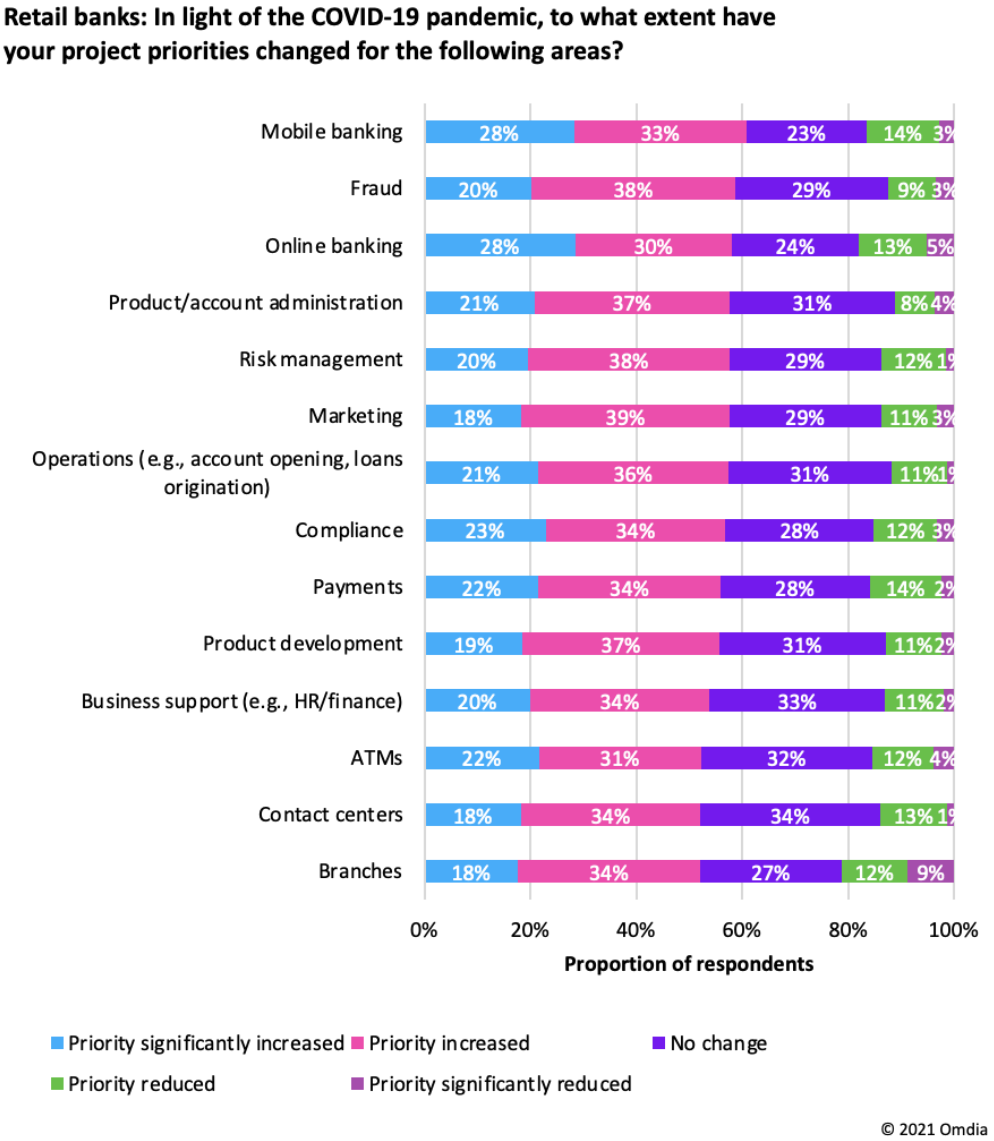
Figure 1: 20% of retail banks cite mobile banking as their top priority IT project



Source: Omdia

Furthermore, as Figure 2 demonstrates, 61% of surveyed retail banks stated that mobile banking projects had increased in priority as a result of the COVID-19 pandemic. This trend was also prevalent among other categories of financial services providers; corporate banks, for instance, were most likely to state that out of all IT projects, mobile banking was most likely to have significantly increased in priority.

Figure 2: 28% of retail banks state that mobile banking projects have significantly increased in importance due to the COVID-19 pandemic



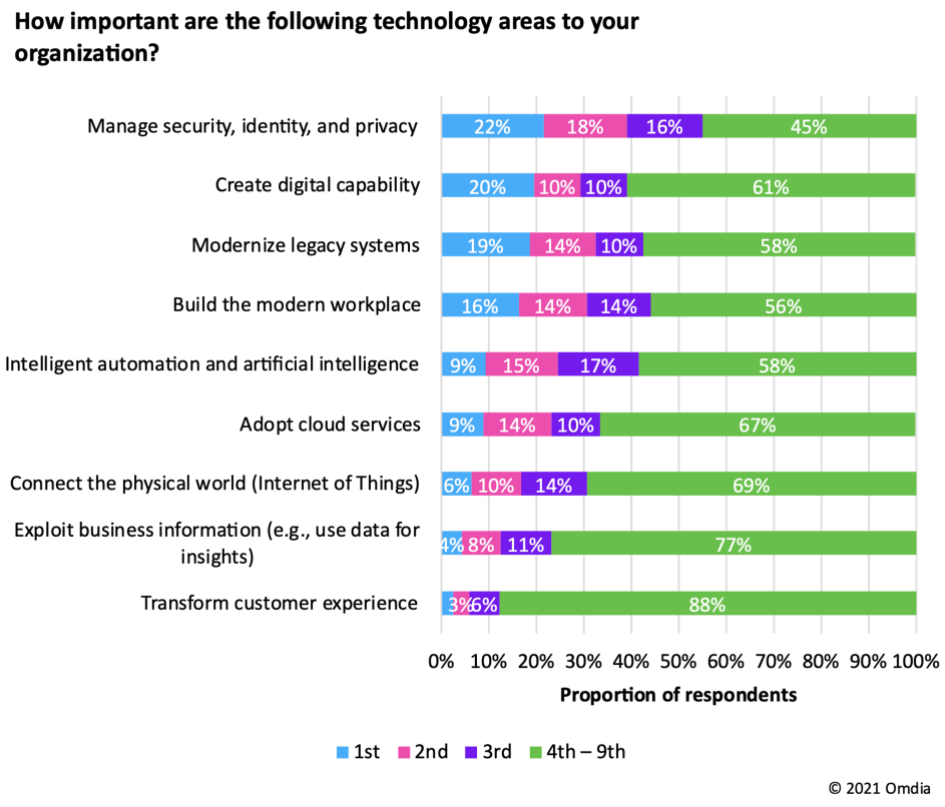
Source: Omdia

Mobile app protection often falls outside of central security

While mobile brings a number of benefits in terms of customer engagement, it also brings a number of new challenges to manage. Security is a case in point; mobile apps provide an entry point to an FSI's wider IT system and, if not protected, can leave the institution open to threats such as hacking. Moreover, it is to be expected that as mobile banking becomes more pervasive, attacks on the channel will increase. Digital channels can be accessed easily from around the world, whereas fraud at branches or ATMs requires a physical presence.

FSIs certainly recognize the importance of security and fraud in their technology strategies, with the theme of managing security, identity, and privacy most likely to be cited as the most important technology area to organizations. 33% of FSIs also stated that this area had become significantly more important since COVID-19, which has brought new security threats.

Figure 3: FSIs place a high emphasis on managing security, identity, and privacy



Source: Omdia

However, while managing security is a key concern to FSIs, mobile app protection can get lost in the organizational gaps between central security teams and mobile app development. Mobile app development typically sits separately to core enterprise technology and security. It is often assumed that mobile security will be managed as part of the app development process, but app developers are focused primarily on core functionality and user experience. Enterprise security teams, for their parts, are typically focused on deploying security measures such as secure servers, firewalls, and pen testing, which are essential for protecting online services, but mobile apps sit outside of these.

Data privacy regulations place the onus on FSIs to protect customer data

The potential for mobile app protection to fall from the radar is particularly concerning given the growing raft of data privacy regulations with which FSIs must comply. These regulations typically demand that companies that control and process personal data also have in place the appropriate infrastructure and processes to protect it. The European Union's (EU) General Data Protection Regulation (GDPR), for instance, stipulates that controllers of data, "shall implement appropriate technical and organizational measures" to ensure processing of data is carried out in line with the regulation. In addition to GDPR, there are also a growing number of national data privacy regulations, such as Brazil's *Lei Geral de Proteçao de Dados* (LGPD) and South Africa's Protection of Personal Information Act (POPIA), which both came into force in 2020 and make similar provisions.

Alongside these overarching data privacy regulations, financial services companies also have to be compliant with industry-specific regulations that also make provisions for security and the management of customer data. For example, the EU's Second Payment Services Directive (PSD2) has a number of security requirements for the processing of electronic payments and also requires alignment with GDPR for data processing. A further example is the Payment Card Industry (PCI) Security Standards Council, which administers the PCI Data Security Standard that businesses handling payment cards from the major schemes have to adhere to.

The challenge for FSIs in managing compliance with these regulations is that they typically detail what should be protected but do not explicitly set out how. The Monetary Authority of Singapore's (MAS) technical cyber-hygiene requirements for different FSIs are one notable exception but, for the most part, country regulators have not taken a prescriptive approach and have left the technical requirements open to interpretation. As such, the onus is on FSIs to determine the best approach to data protection. The risks of noncompliance include hefty fines, not to mention reputational damage.

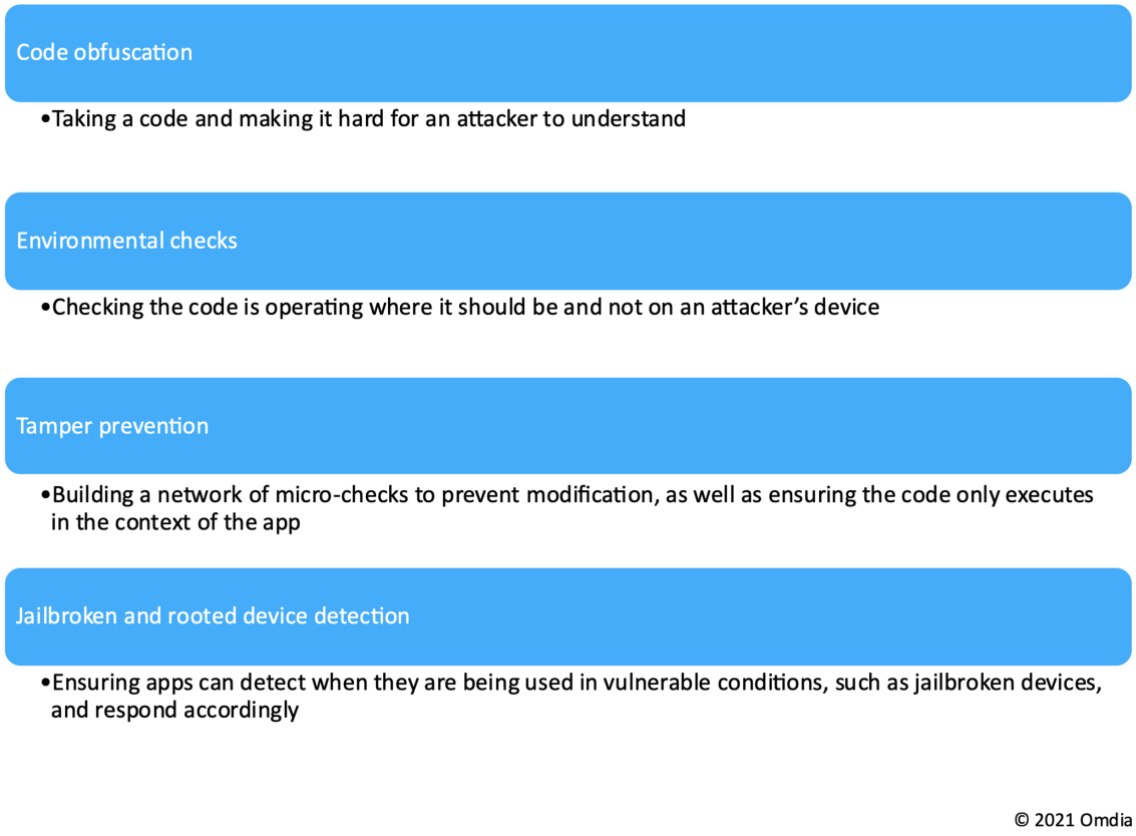
FSIs can ensure full protection of mobile apps by following key practical steps

Ensuring mobile app protection need not be a lengthy or overly onerous exercise. In following some key practical steps, FSIs can ensure apps are protected and significantly reduce the risk of hacking, data breaches, and the resulting fallout these events can bring. From a technological standpoint,

employing automated security tools can enable apps to self-defend against external risks and provide an effective approach to app shielding.

Often, a cybercriminal's first line of attack is to analyze code and gain an understanding of app logic. As such, FSIs need to consider how to protect an app's code to prevent hackers analyzing and modifying it. In doing so, FSIs should look to solutions that utilize a range of defensive techniques to ensure optimum levels of protection. Figure 4 details some of the most important defensive techniques that can be employed, including code obfuscation, environmental checks, jailbroken, rooted device detection, and tamper prevention.

Figure 4: Key defensive techniques for protecting mobile app codes



Source: Omdia

In addition to protecting code, FSIs need to protect algorithms and develop secure cryptographic architectures to avoid exposing cryptographic keys, a common vulnerability in mobile apps. To achieve this, FSIs should look to white box development solutions that can generate a unique cryptographic architecture. However, when considering solutions, it is essential to see how keys are managed. For example, many traditional white box vendors unlock the box, which opens up the potential for keys to be shared between customers and implementations. Instead, more modern

providers ensure FSIs remain in control of their own keys; the vendor does not see them and they cannot be shared across implementations.

Traditionally, such security solutions have been delivered using an on-premises approach. However, increasingly, SaaS security options are also available that are just as capable of delivering high-grade security and protecting against threats such as reverse engineering and application repackaging. The obvious benefit of SaaS offerings is that they allow for greater flexibility and allow FSIs to scale and add more apps as required, with the pricing adjusted accordingly. However, they also offer interesting self-serve options; for instance, enabling FSIs to upload an app and receive back a protected version, thus speeding up time to market.

Ultimately, the starting point for a successful app protection strategy lies in FSIs recognizing the growing importance of mobile apps in the financial services ecosystem and ensuring that their protection is factored into their security strategies. If FSIs can ensure this happens, the technological solutions to provide the necessary defenses are ready and waiting.

Appendix

Methodology

Omdia's ICT Enterprise Insights Technology 2020/21

ICT Enterprise Insights presents the data from more than 6,600 interviews of CIOs and other senior IT decision-makers conducted between July and September 2020. The survey covered 60 countries worldwide, looking at industry technology trends across financial services, telecoms and media, public services, utilities, and retail sectors.

The data was subject to industry-leading levels of rigor. Respondents were drawn from pre-qualified CIOs/senior IT decision-makers who then had to clear a series of screener questions set by Omdia. Interviews were conducted in the respondent's native language where English was not commonly spoken and administered online or via telephone. The resulting data was reviewed by Omdia's primary research analysts as well as our sector experts, using quality assurance tools by Omdia.

Author

Helen Allingham
Senior Analyst
askananalyst@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About Verimatrix

Verimatrix (Euronext Paris: VMX) helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered and frictionless security. Leading brands turn to Verimatrix to secure everything from premium movies and live streaming sports, to sensitive financial and healthcare data, to mission-critical mobile applications. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world. Verimatrix helps partners get to market faster, scale easily, protect valuable revenue streams, and win new business.

https://www.verimatrix.com/markets/financial-services/
info@verimatrix.com

Copyright notice and disclaimer