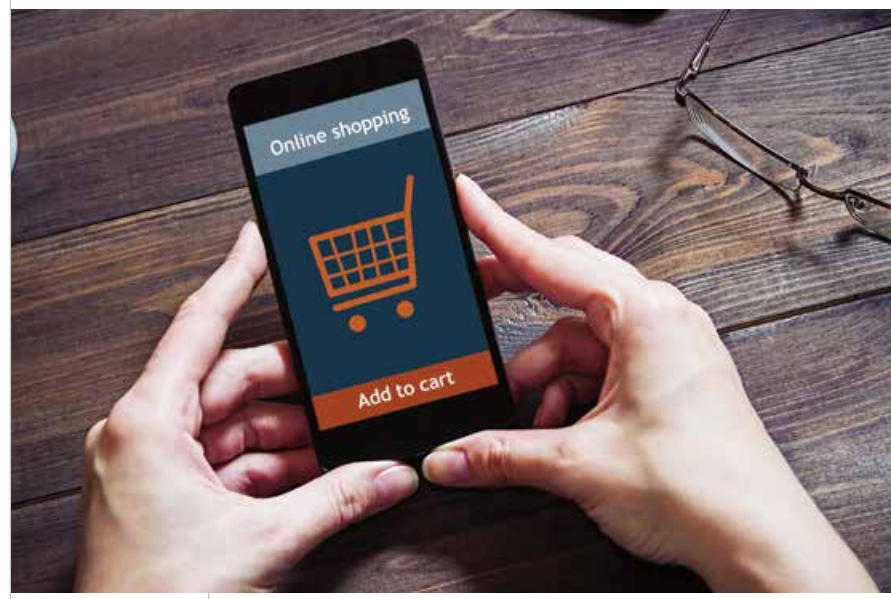
The Rise in Social Media Payments – Will Banks Collapse or Collaborate?

BY FRANS LABUSCHAGNE



As users continue to have frequent interaction and familiarity with social media, it opens doors for them to accept and integrate into their daily lives the financial services these platforms offer. This in turn poses the risk for traditional financial institutions to collapse. Find out in this article the chances and how it can be prevented.

In the last three or four years, social media (SM) giants such as Facebook, Twitter, and Snapchat have harnessed high levels of user trust and engagement to tap into the growing SM payment market. As well as interacting and sharing content with friends, millions of users now utilise these platforms to pay for goods and services and transfer money to one another.

The principles, structures, and technologies upon which SM channels were built have enabled a sharp rise in the success and popularity of their payment offerings. Vast user-bases, inherent interactivity, and an appreciation for user engagement and experience have enabled SM organisations to readily integrate financial services into their platforms. Frequent interaction and familiarity with SM also means that many users have quickly accepted and incorporated these transactional tools into everyday life. The latest annual World Retail Banking Report by Capgemini and banking association Efma revealed that nearly a third of consumer participants are open to receiving financial products from fintech firms like Facebook, Apple, and Google.

However, if consumer trust in legacy FIs is preserved and SM companies fail to upgrade their data security processes and authentication measures, an opportunity for banks to tap into this growing demand for SM payment apps will grow.

Traditional financial institutions (FIs) on the other hand, typically lack these characteristics. Those that are beginning to compete and embrace change are having to overhaul their approach to retail banking and how they interact with their customers in order to catch up to the exponential rise of their SM competitors.

As a result of this upsurge, and the lag felt by traditional FIs, the retail banking sector is undergoing a period of serious and potentially revolutionary disruption. In this state of flux, banks have two options. On one hand, they can combine their strengths with SM companies through collaborative partnerships to create more seamless *and* secure services and maintain long-term growth. On the other hand, they can take no action, lag even further behind, and ultimately run the risk of collapse.

The Collapse of Banks?

While SM platforms are becoming increasingly prominent and useful, consumers are growing disillusioned with the services and experience currently being provided by high street banks. Just over half of the consumers (51%) that were surveyed by Capgemini and Efma researchers said their in-branch experience was positive; only 51.7% were satisfied with internet banking services, and a lowly figure of 47% said they were pleased with mobile channel services.

Ultimately, SM payment apps can offer the type of services and experience that many traditional

banks cannot yet provide. Whereas SM financial facilities emerged as a product of the growing demand for greater convenience and a more personalised, seamless banking experience, legacy FIs are responding to this change in the market and playing catchup as a result.

This shift in demand and customer expectations is, in part, borne from the increasing prominence of SM. We have become so familiar and engaged with SM that we rely on it to facilitate an increasingly broad and diverse role in our everyday lives as both users and consumers. Therefore, as well as possessing the requisite technologies, customer bases, and understanding of user engagement and experience, these apps now inspire levels of trust once associated primarily with traditional FIs and banks.

Bain & Company, the global management consultancy, believe that this increased reliance on SM apps and other fintech companies means that banks are in danger of losing the "special status", as trusted custodians of our financial data and activity. Their survey of over 130,000 banking customers found that companies like PayPal and Amazon ranked nearly as high as banks for trust with money among UK and US banking customers.

If legacy banks and FIs lose this "special status", and fail to modernise their approach and facilities in line with changes in the market, they are in danger of being totally displaced.

Collaboration: Banks and Social Media

However, if consumer trust in legacy FIs is preserved and SM companies fail to upgrade their data security processes and authentication measures, an opportunity for banks to tap into this growing demand for SM payment apps will grow.

At present, SM platforms are facing scrutiny over their ability to protect user information and comply with data protection regulations. Facebook, for example – the biggest of all the SM oligopolies – has suffered a succession of highly publicised data breaches and subsequent GDPR-imposed sanctions, which have generated growing distrust among users.

Security professionals have been raising concerns ever since SM companies expanded into the payment service space. Ultimately, their primary function is to facilitate social interactions between users rather than manage and process their financial transactions. Therefore, users do not always perceive them – and their secondary function as payment services – as a security issue. This can result in negligent security practices, such as using short and memorable passwords and conveniently storing financial and personal information in one place, which makes access to details, accounts, and funds low-hanging (and highly profitable) fruit for attackers.

Moreover, SM apps continually collate and store swathes of valuable user information. Once accessed by a malicious actor, this can be used to carry out social engineering attacks on SM payment apps. Facebook, for instance, generates and stores so much data that a willing adversary can correlate and cross-correlate it in order to posture as a user and dupe others in their network to transfer funds or reveal sensitive financial information.

As SM payment apps client bases grow, and the number of transactions and generation of sensitive financial data multiplies, regulators are likely to intervene to ensure that consumers are protected. This is where legacy banks and FIs could step in. They have a reputation of dependability and security among their customers and the experience and expertise to navigate the complexities of financial regulations that SM companies lack.

It is clear that traditional FIs and SM payment apps have their respective pitfalls. However, it is equally apparent that if they work in partnership, they possess the necessary qualities, expertise, technologies, distribution networks and capital to overcome these weaknesses and provide a service that meets the changing demand of the modern banking customer: seamlessness and security.

SM apps continually collate and store swathes of valuable user information. Once accessed by a malicious actor, this can be used to carry out social engineering attacks on SM payment apps.

Frans Labuschagne is country manager United Kingdom and Ireland at Entersekt, heading operations and business development in the region. He has over 15 years' experience developing and managing technology businesses in Europe, the Middle East, Africa, and Asia-Pacific. Prior to joining Entersekt, he worked in strategic business development and general management roles at enterprise software industry leaders. Frans has broad knowledge of the payments and financial services industries and has participated in a multitude of initiatives across other industry verticals.

References
1. https://www.efma.com/study/detail/28603
2. https://www.bain.com/insights/evolving - the - customer - experience - in - banking /
3. https://www.theguardian.com/technology/2018/oct/02/facebook-hack-compromised-accounts-tokens
4. https://www.cnbc.com/2018/10/02/facebook - data-breach-social-network-could-face-eu-fine.html