FOR BANKING TECHNOLOGISTS

A VIEW ON THE FUTURE OF MOBILE COMMUNICATION IN THE GLOBAL FINANCIAL MARKETS

TRUPHONE

INTRODUCTION

The unprecedented and unforeseen upheaval in the global financial markets has meant financial institutions have been forced to rapidly rethink and redesign their approach to communication globally.

Digital transformation has been on the agenda for at least the last five years. However, through necessity, financial institutions have learned that the habitual, perceived and actual barriers to change can be overcome.

The need and appetite for change is here; it is now time to transform the communications technology underpinning the global financial markets to support the global economy, to compete effectively and thrive in the next decade.

More specifically we seek to consider:

- What is a viable and sustainable mobile device strategy and how can BYOD play a part?
- How can we keep pace with the ever-increasing regulatory demand?
- How can remote working be effectively supported?
- How can supplier controls be effectively managed?
- How can we manage the emergence of Unified Communication?
- How will emerging technologies such as 5G, eSIM and consumer Instant Messaging play a part? And,
- How this can be achieved whilst the industry continues to scale the monoliths of security and compliance, while simultaneously providing the best technology that attracts the best talent and helps them succeed?

This document attempts to take a long-term view on the future of mobile communication in the global financial markets.

To achieve this, we would like to start by considering the key communications and technology trends that have shaped the global financial community, where those trends still apply today and, crucially, how they drive a strategy for the future.

STARTING WITH THE DEVICE

One of the fundamental changes that we've seen affect the adoption of technology is a massive acceleration in the power, capability and extensibility of mobile devices.

In 2010, anyone working for a bank or financial institution had a BlackBerry—a singular, de facto, communications tool for the financial markets. It held great appeal within this community for both its security and its ubiquity: not only was it well accepted by the employee, its closed-source platform ensured that end-user behaviour was secure, predictable and relatively controllable.

Employers were assured that, while it handled voice, messaging and email very efficiently, as long as the enterprise controlled the mobile estate and it was locked into a specific ecosystem, they were safe and secure. Almost the entire industry adopted it.

Contrast that with 2020. Two players – Android and iOS – have swept the board and now dominate the consumer smartphone market, in itself still relatively nascent at the beginning of the decade. Both of these platforms, in their own way, have succeeded in putting extra-ordinarily powerful communications and computing devices directly into the hands of employees, dramatically impacting the control of the employer.

Their domination is due, in large part, to the detachment of and alliance between the software platforms, the applications they support, and the hardware (the handsets themselves) on which those platforms run.

Device manufacturers had to make a tough call: jettison their own operating system in favour of Android or suffer market decline at the hands of those that had. And, as the market leaders – BlackBerry and Nokia – clung onto their entirely closed ecosystems, they quickly lost dominance to wider device choice on the one hand and rapid massive scale application development on the other.

For enterprises, especially those in the financial markets with large corporate mobile estates, this posed three key challenges. The first was the loss of a common, standard device—revered by security and compliance managers within those organisations. The second was cost: if BlackBerry was no longer an option and iPhone or Samsung became the standard, unit prices were likely to increase from £200 to at least £800. Finally, and most importantly, was expectation. As the smartphone penetration in the consumer market grew, thanks in part to Mobile Network Operator subsidised funding, the employee's reliance on its employer for their next new whizzy mobile device rapidly declined.

Indeed, the last decade has shown how hard it is to predict where an industry will be in 10 years' time. And, the past year has proven it can be equally hard to predict as far as 10 weeks! We know we are in the maelstrom of rapid changes but we don't yet know how great the impact will be on the banking industry. As digital transformation is driven more by necessity than strategy, rapid innovation and adaptability is the key to survival. This has created a huge challenge for banks and financial institutions as they plan their technology infrastructure and mobility strategy.

THE MARCH OF TECHNOLOGY CONSUMERISATION

In 2010, corporate IT was in complete control of a specialised and centrally-managed eco-system that developed over decades. Mobile innovation meant that more could be done on the move but, fundamentally, the core systems were trading turrets and MS Office, alongside Bloomberg and Reuters Terminals—all residing on the trading floor. Even the most popular corporate mobile brand – the BlackBerry – ran information through centralised, physical services with its encryption-first, enterprise level capabilities.

All of this was within the absolute control of the enterprise itself. This control gave banks a great deal of security but it did not give the users any flexibility.

Meanwhile, the iPhone was well on its way to mass consumer adoption – this was especially true among the urban elite, many of whom worked in finance. Although it wasn't clear then, that the BlackBerry's time was nearly up. The firm might have created the precursor to WhatsApp with BlackBerry Messenger, but that wasn't enough to fight off a tidal wave of innovation from Apple and Android, and the power of their vast development communities - not forgetting the apparent kudos garnered with the brand association. Touchscreens and 4G gave customers capabilities and functionality not available on their work devices.

Since then, the increasing prevalence and availability of consumer devices has shaken the power dynamic between the IT department and the employee.

This "consumerization" of technology has shifted the power and control from the employer to the employee, who now has access to extraordinary applications and communication tools which are mainly free and all accessible from their device.

With a fleet of communication and research tools freely available on their personal devices, users found they could reach whoever they wanted and find out any information without using their expensive enterprise software on their corporate devices. Moreover, these personal applications were simple to use and did not require the other person to have any specialised communications tools either.

This is probably the most easily demonstrated through mobile messaging applications. In 2010, Bloomberg Messenger was the de facto instant messaging tool for the global financial markets and cost the employer around £1,000 a month per user. WhatsApp and other messaging applications like WeChat or Line, meanwhile, are not only free but also offer a familiar environment as well as several other useful and intuitive features: phone calls, video conferencing, group messaging and file sharing, to name a few.

The consumerisation has meant that as a new generation start moving through organisations, the demands on technology has grown exponentially. They expect applications to offer a great user experience, be able to contact anyone anywhere in the world, be cost effective and – crucially

– available via mobile, to be consumed wherever they are at the time.

This is undoubtedly the trend we will see hardened in the corporate environment in the future and it is becoming all but impossible to overlook. In 2019, for example, one of the world's largest telecommunications organisations failed to recruit a number of graduates to their flagship recruitment programme because the company didn't use Apple. The new generation of talent actually turned down a role because they had to work from a Windows PC.

This is how ingrained the consumerisation trend has become: in order to keep and retain talent, employers are under enormous pressure to enable all these communications tools and must consider that in context with maintaining the high security levels and resilience needed to align with corporate standards.

What's more, this changed landscape means not just a conflict over devices and applications, but also an entirely different spending calculus for corporate IT departments. Providing £1,000 fragile iPhones to the entire workforce can be an order of magnitude more expensive than selectively handing out £200 robust BlackBerrys. They also have to be managed and maintained. With refresh rates between two and three years on average, this represents a gigantic cost to the organisation.

Many employers are therefore understandably keen to explore the benefits of reducing the number of devices they have to procure and manage. One of the options available to them is a policy which allows BYOD (bring-your-own-device) which is a rapidly developing trend in the financial markets.

NAVIGATING BYOD AND CONTROL CONFLICT

It is clear that in order to embrace consumerisation, the enterprise should consider BYOD.

The easiest solution to implement BYOD, one employed by most enterprises that permit it, is to allow employees to use their personal device and personal number for both business and personal purposes, sometimes periodically reimbursed by the company for business airtime and data costs.

In the pure BYOD scenario, however, for all the user flexibility it brings, the enterprise relinquishes all control and oversight over a significant channel being used to conduct its business. The administration of expense claims becomes a challenging overhead and the companies cede all technological and analytical benefits of managing their own estate. The big question for financial institutions – 'how to retain the incredibly high security levels currently enjoyed in a corporate environment on a consumer device' – remains unanswered.

It's unsurprising, therefore that financial institutions in particular have found it challenging to strike a balance between employer authority on the one hand, and user autonomy on the other. Clearly they cannot simply throw up their hands and let chaos rule. Sensitive client and company data is vulnerable to surveillance, leakage and fraud. A balance must be struck between freedom and control. The very difficult cultural and technical challenge is: how can a bank create sufficient functional controls on an end user's personal handset, without creating an anxiety about that user's personal privacy or curtailing personal freedom? Users must have access to relevant corporate applications. Then, as traders, you want them to have timely access to sensitive market data. So how can you give them access to market data, and how can you provide safe access to the bank's market insight on that device?

Thus, the only BYOD programmes that have enjoyed success in the financial markets have been those that implement a containerised business environment within the personal device—delivered via a secure app. In this environment, an area within that handset is controlled by corporate policy and standards. This allows for a segregated component of the personal users' handset that the bank can use to provide its applications, voice communication and data.

The goal is to make it performant, easy and secure while being manageable. Corporations need to understand how to segregate that sensitive corporate data and make sure that the end user cannot go to the corporate side of the device and collect data, and then distribute it from the private side of their device (by taking a screenshot or cutting and pasting, for example). Equally important is removing the opportunity for plausible deniability by making it as difficult as possible for users to 'accidentally' make work calls or carry out transactions from the private side of their device.

One of the greatest challenges at the moment in security is creating that effective delineation. And in regulation and compliance, banks need to convince the regulator and make it suitably clear that, while their method is to have both private and business information and communication functionality on one device, it would be hard for an individual to accidentally make a non-compliant call, or send a non-compliant message.

KEEPING COMPLIANT AMID THIS CHANGE

Over the last ten years, compliance requirements have expanded significantly.

There is a growing conflict occurring between the demand of the users to have all these incredible tools, and demands of regulators for supervision and control. Add to this the new impact of working from home, and the pressure this puts on financial institutions to work harder to ensure the appropriate level of controls are maintained.

In the UK, the FSA has informed the market that the new remote working environment does not in any way change the compliant record keeping and supervision obligations of the firms they regulate. This sentiment has been repeated by most financial regulators globally.

Whereas BlackBerry was an extension to someone's working life, new modern technology is creating alternatives to previous devices and applications. The fluidity between someone's corporate and private life is a huge regulatory challenge. The growth of regulation is happening simultaneously with the consumerisation of IT. Whilst the pace might have previously been manageable, Covid-19 has accelerated everything.

The key to success is to assemble a suite of applications that offer the rich data and communication functionality desired by the employee that are
secure, compliant and device agnostic.

THE IMPACT OF COVID-19

COVID-19 has forced business' hand.

It was no longer the case of *'how do we react to and evolve with these trends?'*, but rather *'how do we enable them now?'*.

It changed the conversation to *'what applications and mobile devices can we rapidly provide securely to enable employees to continue working from home?'*

In short, the banking industry has been forced to adapt to remote working. Where for many, digital transformation had been an aspiration, it is now a necessity and, the market has responded well.

Whilst it's easy to foresee some challenges created by devices and applications, more unexpected challenges have been exposed. On-premise effectively provided infinite bandwidth and full redundancy, but now people's home broadband and GSM connectivity is a key factor in their ability to work from home effectively. Wi-Fi, in particular will start to throw up security and confidence concerns as to whether the networks that people are using are safe from nefarious infiltration. In which case, you have people using secure applications, but on their home network which may be vulnerable.

It's easy to think of the banking industry as being slower to enable working from home, but the reality is that COVID-19 has opened the eyes of many industries as to what can be achieved with remote working.

The question everyone is asking themselves are if we are just experiencing a momentary cessation to business as normal, or will remote working and resilience be a mainstay of the "new normal" and even if it isn't, is it not best to be prepared?

The challenge is how the enterprise can give their remote working employees a "close to" enterprise experience whilst remaining secure and complaint. Working within the constraints of domestic broadband and the potential security vulnerabilities.

In response, the market has found ways to manage. Mobile communication has moved from a back-up, convenient support function to a valuable communications channel. Zoom has become the meeting place of choice but is likely to be replaced by Microsoft Teams as Office 365 starts to land, and virtual Turrets from vendors like Cloud 9 have brought the trading floor to people's kitchens. Innovations with WhatsApp recording and other consumer instant messaging platforms will start to come to the fore.

THE ADOPTION OF UNIFIED COMMUNICATION

Unified Communication (UC) has been a part of the financial institutions' communications portfolio for quite some time.

However, the multi-channel rich collaboration environment of the trading floor has slowed UC's adoption for the trading community.

In March 2020, as financial professionals set up shop in their living rooms, spare bedrooms and kitchens, the need for multi-channel communication remained—and arguably increased. UC tools stepped in to meet that need.

The issue with remote working and UC are two-fold;firstly it is another demand on the finite domestic bandwidth resource, and secondly a new communication channel needs to be recorded and surveilled. For regulated users, all relevant communications need to be recorded as more modalities are added.

The challenge therefore lies in both how employers can simplify the capture and surveillance of all channels; and how the recording environment can be standardised to capture these channels in one place, irrespective of the location of the user, the application they are using and the device they choose.

In response to the challenge, a number of compliant recording vendors are developing multi-channel recording and surveillance platforms that enable the monitoring of voice, messaging and data on one platform. Although these products are not fully formed, the desire is there and the market is ready to consume.

THE COMPLEXITY OF SUPPLY

The third-party supplier oversight requirements for financial institutions to regularly audit and scrutinise their suppliers is increasing rapidly.

The new EBA guidelines of outsourcing stipulate that

"Institutions should be able to effectively control and challenge the quality and performance of outsourced functions and be able to carry out their own risk assessment and ongoing monitoring."

The challenge is clear – how can financial institutions meet these third-party monitoring and management demands of the regulator, whilst at the same time respond to the demands of their users and changes in working practices.

This is creating a huge strain on operational teams and a spiralling total cost of ownership for any individual vendor. In light of these pressures, banks are seeking to rationalise their supplier base. A good example of this is mobility, which was traditionally driven by the domestic nature of mobile network operators, and therefore required a separate vendor relationship in each operating country.

In 2019, a tier-one bank successfully reduced its mobile supplier portfolio from 20 to two by taking a different approach.

TOOLS OF THE FUTURE

The advent of 5G will create new challenges and opportunities for secure connectivity. Native 5G is still years away from being sufficiently ubiquitous for sole adoption, but we need to understand how it fits into the communications ecosystem. We need to explore how this helps smooth the path to BYOD and secure, remote working, without impinging on the personal use of a personal device. The emergence of mainstream smartphones with eSIM as standard will see further benefits beginning to come into fruition, such as the ability to have a second number on a single physical device, or just to have more flexibility in consuming carrier services. The prospect of instant connectivity delivered digitally, over the air, within moments globally is potentially ground-breaking.

Furthermore, the concept that an application could be enabled with its own eSIM connectivity instantly provides a great deal of food for thought. However, eSIM will not become mainstream until it can be enabled with the Mobile Device Management controls the financial institutions expect and need. There are new technologies that help achieve compliance so that consumer apps and devices are recordable and manageable within a corporate environment. If history teaches us anything, it is that trends that start in the consumer world will infiltrate the corporate world eventually, and of course, that's true for technology. If the second decade of the millennium was all about the consumer technology push, the third decade should be about removing that tension and giving corporates more control again while retaining personal freedoms.

But what happens when native 5G is ubiquitous? Will we ever make a GSM voice call again? As applications become the primary communications interface and voice over data is in High Definition, what becomes of the mobile number? Why do we need a mobile number when we have an email address, a Teams account, a twitter handle, are a Bloomberg user and a LinkedIn subscriber?

ABOUT TRUPHONE FOR FINANCE

As the global market leader in compliant mobile communication, Truphone has been supporting the global financial markets for the last 10 years.

Aligned to this, Truphone's revolutionary strides in eSIM technology and unique centrally controlled globally distributed mobile network ideally positions it to support the global financial market for the next 10 years and potentially beyond.

The financial markets have very specific requirements. The demands from both regulators and the business are continually in conflict, and the security regime that must underpin all of this is becoming increasingly onerous.

Truphone believes there is now a requirement in the global financial markets for a global innovator and supplier of wireless communication technology. It launches Truphone for Finance, a specialised full-service connectivity suite, to address this requirement.

☎ +44 20 3002 6565 ✉ T4F@truphone.com 🌍 truphone.com

TRUPHONE