sequent

Trust, Security and User Experience

New currencies emerge - the race is on to remain relevant!

Summary

Banks around the world must now walk a fine line. On one hand, they must innovate to compete and stay relevant to customers. On the other, they must maintain strict security levels as cyber threats and fraud rise with the digital current.

New, valuable currencies are emerging in this continually transforming marketplace and customers are looking to those who can successfully trade in them. Those who cannot will diminish and fall behind.

This paper looks at the mindset and specific technology banks need to adopt in order to support these three vital currencies; trust, security and user experience.

Contents

Introduction

Currency. The word used to mean money. Now it also refers to personal data. What will it mean in the next ten years? And who will have control of it?

Technology continues to leap forward and individuals continue to up their usage levels as both hardware and software platforms pervade their lives. In recent years, this resulted in the data explosion and the recognition of its business potential and revenue generating power. With Artificial Intelligence becoming increasingly sophisticated and accessible, and with the Internet of Things on the horizon ready to send data touchpoints skyrocketing, the upward trend in volume and value of data will continue. Its strength as a currency is guaranteed.

Attention must now turn to emerging currencies that are springing from accelerating digitalisation, advanced data use, and a global society trying to keep pace. In the financial services sector, within banking in particular, these currencies must be capitalised on.

Why? Because customers have deemed them essential.

Three pressures in particular are forging these currencies:

1. From regulation, and the market's response to it, comes the need to guarantee trust.
2. From digitalisation and innovation, comes the expectation of great user experience.
3. From the proportionate rise in cybercrime and fraud, comes the demand for security.

The question becomes - how can banks prove they're strong enough to operate in these areas now and in the near future?

At Sequent, we believe adopting the right outlook and employing technology capable of supporting these emerging currencies is the key banks need to compete in the financial transaction and management marketplace of tomorrow.

To show you, we first need to jump back and see what set banks on the path to today's pressured environment.

Regulation and innovation collide

For banks, as well other financial institutions, two critical fronts coincided and combined to create the whirlwind of change still carrying them forward; regulation and digital innovation.

The world's financial services industry has always been heavily regulated, and the one constant in the sector is regulatory change itself. However, since the global economic meltdown experienced in 2008, today's banks are more heavily regulated than ever before.

Almost all regulation introduced over the past decade has focused on stopping such catastrophic events happening again; tightening banking operating models around the world. We have seen the Dodd-Frank Act, the Volcker rule, and the Foreign Account Tax Compliance Act (Fatca) exert their power in the United States of America while the likes of Mifid II, Basel III, SEPA, Solvency II and more recently the GDPR, steer behaviour in Europe.

Ten years have passed and the world's financial markets, and the financial institutions that support it, are in a much healthier and relatively stable position. The public debate has changed. Whilst there is still the expectation and demand for stability, consumer behaviour and interest is shifting, brought about in the most part by advancements in technology and how businesses use it for the benefit of their customers.

Digital disruption is here and it is here to stay. It began with the evolution of the smartphone and other mobile devices and has since progressed to wearable technologies. Soon, the Internet of Things (IoT) will take smart products a step further. The disruption comes from the boom in connectivity, accessibility and usability. The consumer culture it is building can be described as 'always on, always connected, always active'. It is one of instant gratification and it is one which business leaders in any sector must adhere to in some way; if not in terms of product, at least in terms of sales and marketing activity. Talk with any C-Level professional and the biggest challenge they face, outside of quarterly numbers, is how to transform and remain relevant in the face of this.

When pressures combine

Inevitably, the two fronts of regulation and digital innovation are entwining further; their natures feeding into each other and forcing an upward spiral. Digital innovation inspires regulation to control its use, the regulation inspires new innovation in products, services and experience, and back round again.

Over recent years European regulators have shown some intent and commitment to help stimulate and facilitate change within the digital arena. A clear example of this has been the GDPR. European regulators woke up to the need to rein in rampant use and potential exploitation of EU citizens' data by organisations as technology allowed for its farming, analysis and inspired action at scale. This scale also exposed people's data to increasing risks of misappropriation and attack at the hands of criminals. The GDPR went live on 25th May 2018 and has been designed to protect the personal data and data rights of European citizens.

Businesses and institutions have been obliged to respond to GDPR regulations or face heavy consequences. Innovation has ranged from customer data preference centre development to complete commitment to privacy by design across operations.

For the Financial Services sector the innovation will not stop there. On the regulatory front, you could argue that the GDPR, although not focused solely at the Financial Services sector, is part of a suite of European legislation that is looking to open up the retail banking market across the European Union and the wider European Economic Area.

Couple the GDPR with the revised European Payments Directive, known as the Directive (EU) 2015/2366, or better known as PSD2, one can start to see the regulatory pieces align to drive a change across the European Payments market. Change will demand innovation from banks and financial service providers.

What is PSD2

On 8th October 2015 the European Parliament adopted a proposal from the European Commission. It proposed to increase pan-European competition and participation in the European payments market; opening the door to what has been a bank monopolised market by allowing non-bank providers to participate. At the same time it seeks to harmonise the protection, rights and obligations of both the payment providers and consumers. Directive (EU) 2015/2366, the Revised Payment Services Directive, or PSD2, was born.

The PSD2 provides the regulatory framework to revolutionise the European payments industry and with it, through the ripple effect, global markets. The PSD2 has the potential to impact all forms of payments; from the way we purchase goods and services online to the way we purchase our weekly groceries at the supermarket, pay for our holiday or buy a new car. PSD2 covers all types of payment accounts including current accounts, flexible savings accounts and credit cards. The legislation affects everything from the device we use to pay to the information we see and exchange in order to affect the payments.

Implementation of the new directive will not come without cost but neither does any major transformation or change management initiative.

Regulatory disruption

How does the PSD2 put pressure on banks?

With the PSD2 comes the entrance of two new providers into the European Payments market; Payment Initiation Services Providers and Account Information Service Providers:

- **Payment Initiation Service Provider:** This new market participant is the provider of software that connects the merchant (traditional payee) and consumer (traditional payer). Software solutions look to verify to the merchant that the funds required to pay for the goods or services are available on the consumer's account. The Payment Initiation Service Provider's software then also initiates the transfer of these funds to the merchant.
- **Account Information Service Provider:** This new participant is an aggregator of information from one or more bank accounts of a user. Think of personal financial management platforms offered by some banking brands today, such as: RBC's myFinance Tracker, Standard Chartered's Moneythor, FirstDirect's Internet Banking Plus or F&M Bank's Squirrel

For the first time, there is the potential for non-banking firms to insert themselves into the mix, disrupting the traditional bank-to-customer dynamic. There is potential for banks to become disintermediated as both new participants and consumers look to cut out a redundant middleman. However, only time will tell if this is to be the fate of banks. One thing is certain – failure to react or innovate in the face of this changing market will likely send some of the more traditional banking brands the way of Woolworths, Blockbuster Video and C&A.

PSD2 legislates that the European banking community will have to allow these new market participants access to integrate with their online and mobile banking platforms and applications. If the consumer has provided their consent, then banks will have to grant access to their customer's account information. The establishment and maintenance of trust across all relationships will be essential for this to work.

Open banking and the need for trust

PSD2 isn't the only piece of legislation designed to spur innovation. Another example can be seen in the United Kingdom with the country's 'Open Banking' initiative.

Open Banking is an initiative led by the UK's Competition and Markets Authority (CMA)[1]. The CMA has regulated that the nine largest current account providers in the country (Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds Banking Group, Nationwide, RBS Group, Santander) open up their data via a set of secure application programming interfaces (APIs).

Since March 2017, these nine banks have been working with regulators and the FinTech community to build a standard suite of APIs that allow for the sharing of bank account data. The FinTech community are able to leverage these APIs and develop new and innovative mobile and web-based applications.

Reviewing a 2015 article from the FT[2] it is easy to see some of the potential use cases for PSD2. The article highlights that over 25% UK citizens, 62% in Germany, 40% in Italy, 43% in France and almost everyone in China and Japan with 94%, have relationships with more than one bank. The potential for consumer benefits are easily imagined and that is the ultimate purpose of the PSD2.

For example, a bright FinTech company might develop a mobile app that monitors all of the current accounts, savings accounts and credit cards belonging to a consumer. Whilst monitoring the technology they may see an opportunity to save the consumer money, e.g. by pooling balances from low interest bearing accounts into a savings account or clearing a balance on a credit card so that interest payments need not be incurred.

It goes without saying that the consumer would need to grant permission, to opt-in. Additionally, sensitive bank account and credit card information would need to be stored in the third-party application. Once again, trust is fundamental.

As you can see, whether it be PSD2 or Open Banking, regulations look set to alter and improve the way we bank, in ways we haven't even considered as yet. Changes to regulation provide fertile ground from which beneficial innovation often springs. So too does advancement in technology. Although for traditional banks this hasn't been an easy pressure to adjust to.

1 *https://www.gov.uk/government/organisations/competition-and-markets-authority*
2 *https://www.ft.com/content/c814328c-2bc0-11e5-8613-e7aedbb7bdb7*

Legacy burdens

One of the biggest inhibitors to change is the burden of legacy. The legacy of bricks and mortar branches, the legacy of monolithic, aging core banking and technology infrastructures. Outside of the non-banking threat, there is also the rise of the challenger and online or mobile app-only banks to contend with.

Firms such as Atom Bank, Starling Bank and Monzo in the United Kingdom aren't saddled with history and are able to start with a blank canvas on the reputational and technological front. Their advantage is that they can build their systems infrastructure from scratch and build their business model around current consumer needs versus having to maintain a sprawling mass of legacy.

The end of 'cradle to grave' banking

Yet despite legacy weighing down traditional banks, they are moving forward towards a digitalised world. They have to, as a force just as powerful as regulation, if not more powerful, compels them; consumer behaviour.

Traditionally, a banking relationship with a consumer has been 'cradle-to-grave' with consumer mobility being incredibly limited. Low levels of consumer churn are unsurprising given the laborious process that was, and still is, required in some geographies to switch banking service provider.

Gradually, the Financial Services sector has come to respect the fact that the ability for the consumer to exercise choice is a key driver of effective competition in any market, including banking. If consumers can switch providers, then providers have a much greater incentive to improve their products and services in order to attain and retain customers.

Some countries have set about removing some of the barriers preventing consumers from exerting their power of choice, such as the UK banking market and the Current Account Switch Service (CASS) that was launch in September 2013. CASS is a voluntary scheme which was set up by the Payments Council. The scheme has over 40 bank and building society brands participating, covering over 99% of the UK current account market. It makes switching current accounts simpler and quicker for retail customers, some small businesses and charities.

The cradle-to-grave mindset is changing. New technologies are obviously playing a dominant role in disrupting the value proposition of established payment products. Credit and debit cards have become run of the mill; in the UK there are over 98 million debit cards[3] in circulation. Internet connectivity and mobile access through smartphones and other devices is contributing to the crumbling of traditional banking operations. Specifically, through their ability to enable consumers to conduct transactions and financial management through the tap of a finger.

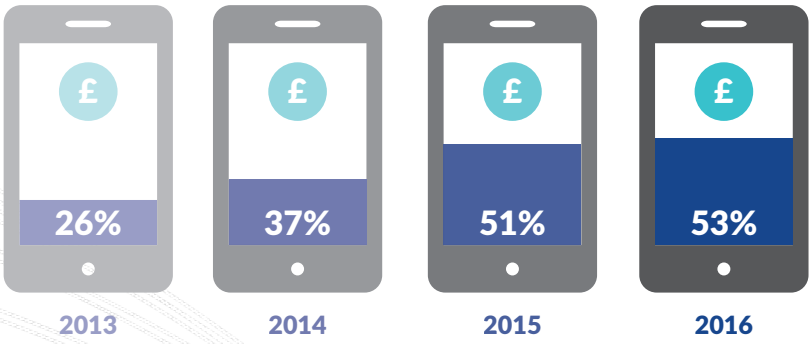
3 *https://www.ukfinance.org.uk/wp-content/uploads/2017/12/9.-Debit-Card-Report-October-2017.pdf*

Digitalisation is the new norm

Consumer behaviours continue to change, thanks to technological capability, and online spending continues to grow. Commoditisation of the personal computer and accessibility to information at any time of day, the ability to shop at one's own convenience rather than being constrained by store opening hours, has all been instrumental in driving change. Add to this the proliferation of the smartphone and we see the consumer has more power and more convenience than ever before.

In 2016 53% of UK consumers online spend was conducted on a tablet or smartphone. The consumer's palm now holds tremendous power.

Spending channelled via mobile devices



(source: The UK Cards Association)

Changing consumer purchasing habits bring new challenges that require new innovations in several areas. Banks, credit card companies, card issuers, card schemes, merchants, acquirers and third-party payment services providers have all had to walk a tightrope of offering choice, convenience, security and consumer protection that matches consumer expectations of user experience.

First, we saw new security factors to support and replace the traditional magnetic strip and signature when EMV chip and PIN card technology became mainstream in Europe in the early 1990's. Chip and Pin meant the consumer's money was safe, even if they lost their card.

However, this wasn't enough as the evolution of the smartphone and tablet brought with it the concept of the mobile wallet which would require its own stack of innovation to cover personal protection. The mobile wallet is a means of carrying the traditional plastic card in a digital form on a mobile device. When we say 'plastic card', most people will naturally think of a credit or debit card, but our thinking of it and conversations should also incorporate things such as brand loyalty and travel cards.

The mobile wallet allows the consumer to make and receive payments using their mobile device and the list of devices is increasing; smartphones and tablets are quickly becoming joined by wearables and even household appliances look set to join the fray as the Internet of Things is becoming a reality. Once, the idea of talking appliances was the realm of science fiction. Soon, the digitalisation of our homes and wider environment will be commonplace.

User expectations

The success of the mobile wallet has so far been limited as consumer adoption and merchant acceptance of new technology takes time. On the merchant side, their dependence on point of sales (POS) terminals being ready for contactless payments has certainly been a limiting factor. On the consumer side, there have been concerns about security and trust as they question how secure transactions are and what happens if their device is hacked or lost.

The mobile wallet is only possible because of advancements in data transmission technologies like near field communication (NFC) and Bluetooth. Both have been instrumental in disrupting the payments landscape and Apple Pay, Samsung Pay and Android Pay all leverage NFC as part of their digital wallet offerings.

The breakthrough for mobile wallets really came in 2014 when Apple launched the iPhone 6. The iPhone 6 was the first Apple device to support NFC technology and, even though Android devices had the capability for a number of years beforehand, set the trend firmly in the public eye thanks to Apple's brand power and marketing. With most high-end smartphones now enabled it was POS technology's turn to step up and from that point on, many stores started to upgrade their terminals.

According to the World Payments Report 2017[4], mobile wallet transactions are expected to grow at a compound annual growth rate (CAGR) of 61.8% during the period 2016 to 2021. It is safe to say that the global payments landscape is evolving at a rapid rate and with the globalisation of ecommerce it is becoming even more complete.

In order for banks to remain relevant and competitive, they must understand today's payment trends and consumer needs whilst considering how to advance their payments processes to meet the demands placed upon it by modern commerce. In recent years, the talk has been that banks will soon experience a dramatic loss of market share, similar to that experienced by BlockBuster Video, Woolworths and C&A in their sectors, and that technology firms could displace them altogether.

Whilst the banking industry is challenged by, and has to cope with, legacy issues that impede their ability to react, large parts are being digitalised, especially in consumer finance. Having innovative banks that can offer up-to-date services to their customer base is seen as a prerequisite for the achievement of an advanced digital economy. This is why regulation such as PSD2 is not only a regulatory, compliance and technology challenge, but a strategic and operational opportunity.

Consumers already see the digital user experience as an attractive currency being used by businesses. Banks should be focusing on technologies and applications that demonstrate care and consideration for the modern consumer as expectations of the banking experience will continue to increase in terms of convenience, sophistication, personalisation and security.

Security is the third and final emerging currency we must discuss as explosions in digital ingenuity don't just occur within legitimate businesses, such as banking. There is another powerful group in society also benefitting from rising digitalisation – criminals. This group applies its own very specific pressure on banks and their consumers, and is the explicit generator of security as a currency.

4 *https://worldpaymentsreport.com/*

Fraud and cybercrime

The rise of digitalisation in the banking community has a dark side; the cybercriminal. No longer does the bank robber need a balaclava and a gun, today they just need a computer, time and perhaps caffeine.

Financial crime has always been an unfortunate feature of society, with criminals usually targeting the weakest link in the chain. In the days of bricks and mortar banking this was the branch teller but with advancements in technology criminal behaviours have changed. The end consumer has become the target. Card fraud and account hacks are now all too common. As financial services firms innovate so too does the criminal. There are already studies exploring how artificial intelligence and machine learning can be applied to create a master fingerprint that will be able to open any personal lock.

In a recent survey in the United States, conducted by Experian[5] , it was found that 55% of consumers preferred to use traditional credit cards rather than a mobile wallet because of security concerns. In a separate survey of consumers based in the United States, the American Bankers Association found that although 25% of consumers have made a payment using a mobile device, only 12% trust alternative payment providers to be able to secure their data and payment details.

Trust and security has become a new battle ground for the banking industry and it's a battle they must win if they are to retain happy customers. Globally, e-payment volumes continue to increase with consumers transacting more of their banking activity online and via mobile devices. Convenience has become a must for consumers. They want the 'Uber' experience from their banking providers.

However, rapid changes in the digital world and the desire to meet consumer expectations needs to be tempered with security considerations. It is a world in which security can't be neglected or overlooked; the ability to detect and prevent cybercrime is critical to retaining the trust of the consumer.

The global cost of cybercrime will reach $6 trillion by 2021, [6]a **threefold increase** from the 2015 estimate of $500 billion.[7]

Globally, cybercrime was the 2nd most reported crime in 2016.[8]

PwC's 2018 Global Economic Crime and Fraud Survey finds that 49% of global organisations say they've experienced economic crime in the past two years. **Up from 36% in 2016.**

Software update supply chain attacks *(implanting malware into an otherwise-legitimate software package)* were **up 200% in 2017.**[9]

Mobile threats continue to grow, including the new mobile **malware variants up 54% in 2017**. Symantec blocked an average of 24,000 malicious mobile applications each day last year.

70% of all financial fraud in the UK in 2016 was transacted through remote purchases using stolen information.[10]

More than 60% of fraud originates from mobile devices. It used to be mobile browsers that were fraud heavy, now **80% of mobile fraud comes from mobile apps**.[11]

As consumers migrate more and more of their personal data and purchasing habits to the mobile channel, the cybercriminal lays in wait. As more and more banks and merchants increase the range of products and services on their mobile apps, targeting the mobile channel is a natural shift for the cybercriminal. In the United Kingdom in 2018, £1 in every £3 spent was spent online. That's a big pot for criminals to target. With the drive to open up the banking networks and the rise of open API's fuelling innovation in the banking sector, the opportunity for the consumer to be a victim of cybercrime increases with it.

5 *https://www.cnbc.com/2018/03/02/digital-wallets-are-safe-yet-americans-remain-wary.html*
6 *https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/*
7 *https://securityintelligence.com/20-eye-opening-cybercrime-statistics/*
8 *https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html*
9 *https://www.symantec.com/security-center/threat-report*
10 *https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/Fraud-the-Facts-A5-final.pdf*
11 *https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf*

Recent attacks

There have been several high-profile data breaches and distributed denials of service (DDoS) over the course of 2017 and 2018.

The WannaCry ransomware attack in May 2017 impacted over 150 countries and 200,000 computers, as criminals demanded each of those affected pay up to $300 worth of bitcoins to unlock their systems.

The British Airways hack was another high profile attack that occurred in August 2018. This breach saw cyber criminals steal personal and financial details of people who had booked flights on BA.com or the companies mobile app. [12]This hack affected around 380,000 BA customers over a 15-day period. The BA hack saw customers name, addresses, debit and credit card details placed at risk, including card numbers, expiry dates and the card verification value (CVV), compromised. With this information a cybercriminal could clone the card and make online purchases or sell the information to other criminals.

Card fraud isn't confined to one country or one region. It is happening globally and at extremely high levels. It places a significant burden on the banking community, financially, making cybersecurity a top priority for banks, merchants and the regulatory community.

If security controls are weak or missing all together, the risk is borne by the bank or firm providing the service and they must ensure they have the appropriate protection in place in order to secure the consumer's personal data and money.

Looking at a 2017 study by CapGamini[13], the highlight is a shocking disconnect between consumers and banks on the level of security in the financial services sector. The survey covered 7,600 consumers and 180 data privacy and security professionals from banking and insurance firms in eight countries. It showed that the banking and insurance sectors have seen trust levels increase post the lows witnessed during the 2008 financial crisis, with 83% of consumers having trust in the cybersecurity of their banking and insurance providers systems. Yet, industry insiders expressed a contrary view. Just a fifth of bank executives were highly confident that their firm could detect a data breach, let alone defend against it.

There is clearly much work to be done to support security if it is to be a currency banks can trade on.

12 *https://www.independent.co.uk/travel/news-and-advice/british-airways-flights-ba-hacked-data-theft-customers-a8526516.html*

13 *https://www.capgemini.com/sites/default/files/just_one_in_five_banks_and_insurers_confident_they_could_detect_a_cybersecurity-breach.pdf*


CyberAttack
Crime
Data

New currency mindset

As banks come under pressure to stay competitive and open their systems, consumers will begin connecting their bank account to other services and other aggregators, benefiting from the convenience of single sign-on to view all of their financial activities. Likewise, the growing popularity of the flexibility to move money around at will, whilst on the move, is pushing the market for mobile wallets. Underlying all of this is the potential for fraud and cybercrime if proper security is lacking.

Banks must be able to trade on trust, user experience and security with confidence. To do so takes two things; a distinct shift in mindset and the adoption of robust technology.

The right mindset is one which accepts that digital transformation is no longer merely a nice to have for banking and the wider financial services sector. It is crucial and will be how the likes of the banks, insurance firms, and credit card schemes are going to keep pace with consumer demands and expectations. Resistance and a clinging to old operational models will bring companies down.

There are many examples across all industries where once household brand names have met their demise due to a lack of innovation; fading from relevance, being swallowed up by stronger competitors or simply ceasing trading altogether.

Woolworths, the British high-street retail chain, whose major business activity was selling music CDs and DVDs, failed to adapt to a consumer base making the shift to streaming. Woolworths stopped trading in 2008. 2010 saw a similar story in the US with video rental chain Blockbuster Video. In the world of technology, Nokia, the company that built prototypes of touch-screens and internet enabled phones at the end of the nineties is suffered a similar fate. Once the dominant player in the fast-paced mobile phone space now is nowhere to be seen. Nokia invested in innovation, but what they lacked was the ability to translate that research and development spend into products that people wanted to buy.

Yet doom and gloom is largely reserved for those unwilling to seize upon change and move with digitalisation. There are plenty of companies that have innovated and kept one step ahead. Amazon is the obvious example. Back in the spring of 1994 Jeff Bezos began to see the internet revolution taking place with web usage growing at 2,300% per year. It was the trigger for him to start his own internet company. Amazon started as an online library selling books, as books were low cost and there was universal demand. Fast forward 25 years and Bezos' Amazon is now the largest retailer and logistics company.

Embracing digital disruption will take banks further than protecting against it. Regulation and subsequent technological innovation means it is inevitable. The question is – how much are banks willing to change in response to it? Given the risk averse nature of banks, coupled with stricter regulations, the thought of wild experimentation with new technologies and operating models can bring executives immense anxiety.

One answer is to look at current technology that can underpin a secure move towards what customers want and expect while guaranteeing security. The technology? Tokenisation.

New currency technology

With trust, user experience and security becoming the new currencies with which to buy consumer loyalty, banks are increasingly turning to fintech partners and their technological solutions in the fight to provide great service and tackle things like payments fraud.

As we have seen throughout this report, the payments landscape is ever-changing, driven by consumer behaviours, regulation and technology advancements. To stop cybercriminals, who are evolving and adapting to new technologies just as quickly as industries innovate, the banks and payment service providers need technical solutions that:

- Are easy to deploy, manage and upgrade
- Evolve at a rate as quick, if not quicker, than the cyber criminals can adapt
- Reduce costs

In the payments landscape, cards tokenisation on the mobile device is a means to manage these three elements at the same time, making the traditional plastic card digital and easy to use by consumers.

Tokenisation platforms empower banks, transit agencies, access control providers, and any other card issuer, to securely digitise their credit, debit, transit, loyalty, or ID cards; distributing them to their own application, or any others, using the technology partner's platform.

Best-in-class tokenisation platforms require three core components:

- Token Service Provider (TSP)
- Card and Wallet Management Platform
- Trust Authority

Tokenization becomes the definitive weapon against the cybercriminal, being able to replace sensitive information with data that has reuse value if it falls into the wrong hands. Tokenization is the next generation of security for the modern, highly connected, mobile world, and is just one example of the innovation required.

Conclusion

Digitalisation is occurring in the banking industry, and especially the payments market, with or without the banks blessing. Traditional banking brands are saddled with legacy infrastructures and are not adapting effectively enough. Changes to regulatory environments and advances in technology have empowered new entrants and new technologies to enter into the market. With consumer behaviour changing and with trust being built with large technology brands, banks risk being disintermediated from the payments arena if they don't refocus.

Banks can only be truly flexible if they work with flexible partners. Service providers must be able to accommodate banks' evolving requirements in an evolving landscape. Only then can banks make the most of these new currencies bubbling up from modern pressures and appeal to customers whose financial service options are about to blossom.

Wherever innovations come from, no matter how they are done, one thing is clear, banks need to continuously innovate in the areas of security and user experience in order to remain relevant and build trust. To fail to innovate is to risk commercial death.

About Sequent Software Inc

Sequent Software Inc is a leading provider of tokenization solutions that secures data on the move. Sequent's Platform brings cards to mobile and makes them useful for consumers. Sequent enables banks, transit agencies and any other issuer to securely digitize their credit, debit, transit, loyalty or ID cards and distribute them to their own application, and to any other application using the Sequent Platform. Sequent's simple APIs empower the app developer community to bring cards to all apps on mobile, wearable, and other connected devices enabling consumers to make payments, redeem offers, open doors, and ride transit systems. Sequent Platform includes: Token Service Platform (TSP), Card and Wallet Management Platform, and Trust Authority.

Contact us

Sequent Software
4699 Old Ironsides Dr. #470
Santa Clara, CA 95054

info@sequent.com

www.sequent.com