THE FINTECHTIMES.COM

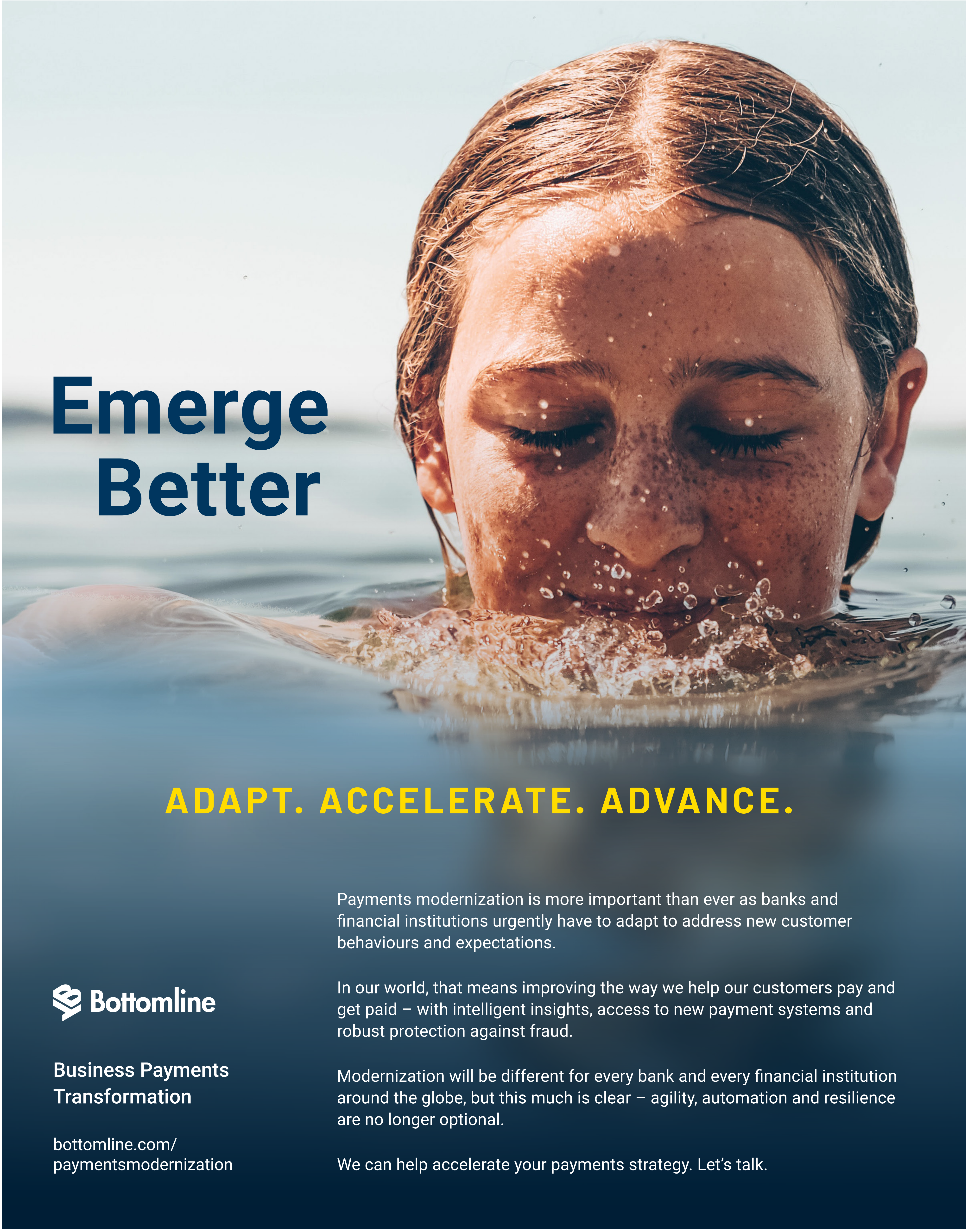
EDITION 36

THE FINTECH TIMES

THE WORLD'S FINTECH NEWSPAPER

INDUSTRY EXPERTS OFFER CYBERSECURITY ADVICE FOR A COVID WORLD

IN THIS ISSUE


Emerge
Better
ADAPT. ACCELERATE. ADVANCE.

THE FINTECH TIMES

BRINGING FINTECH TO THE WORLD

Editorial Enquiries
editor@thefintechtimes.com

Chief Executive Officer
Jason Williams

Editorial Director
Mark Walker

Business Development
Deepakk Chandiramani
Sally Gensberg
Steven Jones
Terry Ng
Ania del Rosario

Editor
Claire Woffenden

Editor-in-Chief
Gina Clarke

Art Director
Chris Swales

Digital
Manisha Patel

Junior Journalist
Polly Jean Harrison

DISRUPTSMEDIA
LIMITED

Published by
Rise London, 41 Luke Street
London EC2A 4DP
United Kingdom

CONNECT WITH US
/fintech-times
/thefintechtimes
/thefintechtimes
thefintechtimes.com

This Newspaper was printed by
Park Communications Limited,
London using its environmental print
technology, on 100% recycled paper.

THE IMPORTANCE OF CYBERSECURITY

In 2020, fintech experienced an unexpected demand for services with many organisations forced to move away from more traditional business models to accommodate the demand for services available online.

But while new technologies enable greater connectivity and open up exciting opportunities for growth, they also bring systems that attackers want to exploit. Over the past year, cybersecurity strategies and practices have been firmly put to the test because even a pandemic can't deter the fraudsters.

Of course, financial organisations have always been a prime target for cyberattacks and ransomware threats with their treasure trove of highly sensitive information and data, but the coronavirus pandemic has opened up even more opportunities for malicious hackers and criminals to exploit individuals and businesses as they get to grips with disrupted routines and new ways of working.

A Covid-19 disrupted world has led to proliferating social engineering opportunities and put pressure on organisations struggling with business continuity, travel restrictions and remote working and the pressure to accelerate digital transformation plans.

An increased level of sophistication makes cyberattacks much harder to identify and more threatening. Cyberattacks, especially against banks and those working in finance, have increased dramatically since the start of the coronavirus pandemic, with a 238 per cent increase in financially motivated attacks, according to the third edition of VMware's *Modern Bank Heists Report*.

An increased level of sophistication makes cyberattacks much harder to identify and more threatening

In this issue of *The Fintech Times*, we put the spotlight on cybersecurity, addressing the latest trends and concerns, while discussing how businesses can look to ensure both their employees and customers are kept cyber safe throughout the disruption.

On pages 4 to 5, we hear from security experts from across the financial industry on how cybercrime is evolving in response to the Covid-19 pandemic, as well as the benefits of community and culture.

Nicolai Solling, chief technology officer of cybersecurity firm Help AG, chats about the development of increasingly sophisticated cyber threats and the importance of securing the huge amounts of sensitive data that go into fintech as organisations.

On page 16, Chris Ganje, founder and CEO of AMPLYFI, discusses his fascination with analysing the disruptions faced by global finance organisations and warns that every branch of an organisation will need to become aware of all forms of cybercrime and cybersecurity.

While Justin Pike, founder and chairman of MYPINPAD, highlights the payments industry's role in supporting vulnerable people, on page 19.

We'd like to take this opportunity to wish all our readers a very happy and healthy 2021. TFT

Claire Woffenden, TFT Editor

FIGHTING THE FRAUDSTERS: A GAME OF CAT AND MOUSE

Cybercrime is evolving in response to the coronavirus pandemic, but so too is the fight back

During the annual gathering of the Association of Certified Fraud Examiners last year, Jean-Francois Legault, MD and global head of cybersecurity at JP Morgan Chase, commented: "If you build a better mousetrap, it's highly likely that an adversary will build a better mouse."

Fraud has always been a cat-and-mouse game, where the good guys try to keep up and ahead of the increasingly sophisticated tactics of the bad guys. But during the pandemic, this battle has intensified.

Coronavirus-driven lockdowns, social distancing and people staying at home, with more free time and more disposable income, has led to mobile apps and online payment tools soaring in popularity with many fintechs reporting tremendous growth. However, just as quick to profit from the pandemic are fraudsters, who have gone where the money is to steal as quickly and easily as possible.

PANDEMIC-POWERED FRAUDULENT ATTACKS

According to fraud fighting firm **SEON**, rather than deterring fraudsters, the pandemic has, in many cases, empowered them. More traffic accordingly means more fraudulent behaviour.

In its latest report, *Fighting the Fraudsters in an Age of Pandemic*, SEON warns that: "As the world migrated online in record numbers to cope with restrictions on physical movement and interaction, within their numbers were those with nefarious intentions. As so much fraud is now perpetrated in cyberspace, many fraudsters saw an opportunity in enhanced traffic volumes, and they have been capitalising on it."

The report highlights that as cryptocurrency and online trading experienced growth during the early months of the pandemic, it also led to a spike in fraud. With sporting events postponed and cancelled, the popularity of eSports and iGaming has also grown – but so too has abuse in the sectors. While bonus abuse, multi-accounting and affiliate fraud were always persistent forms of attack, the popularity boom has also attracted the attention of more experienced and more ruthless fraudsters.

Daniel Sebes, SEON's eSports expert and business development manager, says: "We have found that fraudsters were registering multiple accounts and playing against themselves, using the bonuses provided by operators to generate cold, hard cash."

PHISHING ATTACKS

Security firm **F5** also reports on a drastic increase in phishing and spearphishing attacks. News about vaccines or elections have been leveraged to entice people to open emails from unknown sources, or even known sources who may have had their accounts breached and hijacked, to then spread malware and other malicious attack to steal user and corporate information or enable illicit access to sensitive networks, clouds, applications and data.

Keiron Shepherd, principal solutions engineer at **F5**, comments: "Cybercriminals are becoming very adept at misleading voters with disinformation. This includes propagating false news, using bots to drive social media engagement and the strategic leaks of incriminating emails or confidential documents."

"With data breaches reported on a near weekly basis in the national news, the view around cyber culture has changed considerably over the last few decades. We've gone from lone hackers in bedrooms to nation states weaponising zero-day attacks. More than ever, businesses and individuals are starting to understand that data is a valuable currency that needs to be protected."

ORGANISATIONS UNDER ATTACK

For its *Cybersecurity in the Remote Work Era: A Global Risk Report,* research firm **Ponemon Institute** – commissioned by password manager firm **Keeper Security** – surveyed IT security personnel from across the globe. Its report found that during the pandemic, many organisations have had exploits and malware that evaded their intrusion detection systems and anti-virus solutions – with credential theft and phishing, or social engineering, the most frequent types of cyberattacks.

It was also revealed that cyberattacks during Covid-19 are becoming more severe in terms of negative consequences, such as the impact on finances, with cyberattacks becoming more targeted and sophisticated. Fifty-eight per cent of those surveyed said that their organisations experienced a compromise that damaged IT infrastructure or stole IT assets.

Darren Guccione, CEO of password manager **Keeper Security**, says: "The past year has been a radical, cybersecurity wake-up call for the fintech industry. The pandemic exposed mass ill-preparedness across the entire finance sector with 70 per cent of companies experiencing a cyberattack in the last 12 months. With businesses entering 2021 having to face the double whammy of stringent lockdowns and challenges the new Brexit deal brings, it looks like things will still get worse for the sector on the cyber risk front before they eventually get better."

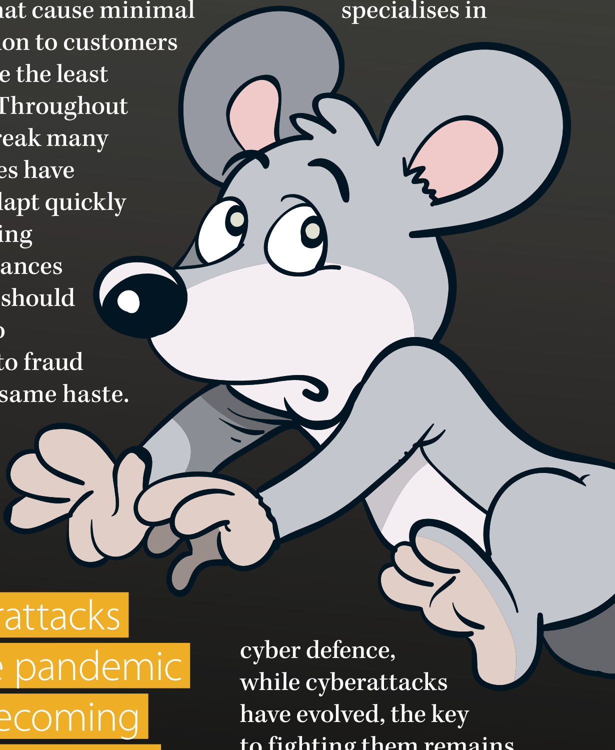
FIGHTING FRAUDSTERS

While the identification of threats is key to understanding exposure and risks, the increase in fraud during the pandemic has underlined the need for communication and collaborative action in the battle against cybercrime.

For **Tamás Kádár**, CEO and founder at **SEON**, it is crucial that businesses don't focus solely on their digital successes during the pandemic.

"The online space is busier than ever and companies are looking to remain competitive while they find their feet in the new normal. That being said, it's essential that they don't focus solely on bolstering conversions at the expense of security and vice versa. It is a balancing act. While security measures should be tightened, businesses should be conducting risk checks that cause minimal obstruction to customers and cause the least friction. Throughout the outbreak many businesses have had to adapt quickly to changing circumstances and they should be able to respond to fraud with the same haste.

"It's important to understand that there is no way of fighting fraud that can ever be 100 per cent successful. Every time a company like ours develops a new line of defence, the fraudsters begin looking for ways to bypass it. A solution we develop today might be outdated in just a few months' time. Unfortunately for the fraudsters however, though they may never stop, neither do we."



EMBRACING TECHNOLOGY

For **Darktrace**, an artificial intelligence company that specialises in cyber defence, while cyberattacks have evolved, the key to fighting them remains the same.

Dave Palmer, director of technology at **Darktrace**, says: "Static security – creating rules about what is 'good' and 'bad' simply can't keep pace. There is no silver bullet to cybersecurity but today we have technology available that can stop novel attacks at machine-speed.

Cyberattacks in the pandemic are becoming more severe in terms of negative consequences, such as the impact on finances, with tactics becoming more targeted and sophisticated

Finding the right people with the right skills to defend organisations is important, but they cannot handle the challenge alone. We need to augment teams with AI that can make decisions in seconds."

TAKING RESPONSIBILITY

According to **Tim Hickman**, partner and data protection lawyer at law firm **White & Case**, it is essential for any business to understand its legal and regulatory compliance responsibilities and identify the relevant cybersecurity risks, take a proactive approach wherever possible, and have a reactive plan in place where needed.

Hickman said: "In the wake of a cyber incident, establishing [an] initial snapshot assessment is incredibly important as it will drive not only the prioritisation of the response, but the entire process. If an incident is correctly identified as high risk at the onset, the response timeline will accelerate, with organisational resources deployed more appropriately. Principally, it's about damage limitation and controlling the incident, so understanding the mitigating factors that might help to reduce risk to the business is key."

Chris Huggett, senior vice president EMEA, at IT provider **Sungard AS**, says: "In today's IT-driven business world, assessing technology risks is a critical part of business continuity planning in every company across every industry. This is especially true when it comes to cybersecurity, where even the smallest IT footprint provides attackers with a gateway to global supply chains, and the ability to wreak havoc on countless stakeholders."

LESSONS LEARNED

Meanwhile, **Chris Hodson**, chief information security officer at security and systems management firm **Tanium**, believes that increased threats should be a "timely reminder for business leaders to incorporate resilience into their distributed workforce infrastructure if they're going to manage the security challenges of this new world of work effectively."

He adds: "Many of the issues that emerged at the start of lockdown resulted from considerably overestimating preparedness for the security challenges that came with shifting to a distributed working environment. Our research found that 85 per cent of business leaders thought they were prepared to manage the shift to widespread working from home. This confidence turned out to be ill-founded with 98 per cent admitting they faced security challenges in the transition away from the office.

"Even before the virus emerged, concern among IT leaders was growing with tool sprawl, shadow IT and legacy tech creating a slew of security challenges. Not only did widespread remote working exacerbate these existing issues, it also created a host of new security challenges, allowing cybercriminals to run amok during a period of deep confusion and uncertainty for businesses.

"Whether companies choose to permanently move their operations, return employees to the office, or some combination of both, implementing endpoint management and efficient security solutions should be a priority."

ALLOCATING RESOURCES

Keeper's Guccione agrees that with remote work poised to continue, the fintech sector needs to equip staff with the right cyber defence preparation at home, rather than waiting to reinstate security measures for a return to the office.

"We can expect to see a rise in cybersecurity awareness training and general education covering online security," he says. "Presently, 34 per cent of those in the finance industry have no understanding of how to protect themselves against a cyberattack. The mass handling and management of financial assets makes fintech companies a prime target for cybercriminals. Increased budgets and resources should be allocated in order for fintech organisations to bolster internal controls and effectuate robust cybersecurity and incident response plans. In part, this will involve further investment in identity access management solutions that utilise a zero-trust framework, zero-knowledge security architecture and an enterprise password management platform that can tie into and strengthen their identity applications."

THE FIGHT CONTINUES

Cybersecurity is a never-ending cat-and-mouse game. As new services emerge and preventative technology evolves so too does fraud. Constant fine-tuning of fraud detection strategies and compliance is vital.

Businesses and individuals must arm themselves with the right tools, the right knowledge and be prepared to communicate in order to remain cyber resilient. The fight against fraud will continue... TFT

Bringing the $47trillion retirement market into the 21st century

Richard Dallas, Chief Revenue and Platform Officer at Smart

An alumnus of the London School of Economics and Political Science, with experience across HSBC, Lloyds, Barclays, Aegon Transamerica as well as Starling Bank and numerous startups, ***Richard Dallas*** *breaks down his perception of the pensions and retirement savings market globally, and the 'state of tech' within this Goliath sector of the fintech industry*

THE CHALLENGE, THE BARRIERS AND THE OPPORTUNITY

In the race towards technological transformation, has retirement technology been left behind by the sheer speed of digital change in other areas of our professional and personal lives?

Undoubtedly so. From my perspective, the evidence is clear. Retirement tech is definitely 'behind the curve' of the overall fintech market. We know this from looking at global data from the retirement savings industry, as well as from the more than 800,000 direct members of our technology platform, as well as the information we get from our many partners. But the opportunity for both financial services, and the individual is huge. In this article I want to talk about three things:

1. The widening tech gap in the $47trillion retirement savings industry
2. What's caused that, and why it's relevant now
3. The opportunity: How to fix it, benefiting the finance industry, benefiting the fintech industry specifically, and benefiting billions of people worldwide

The first of my personal triggers for writing this article, is something fundamental. The retirement industry has failed to innovate for the benefits of consumers in the run up to and during retirement. The amount of time taken to innovate in this area is simply too long, at a time when hundreds of millions could benefit from that innovation today.

The second of my personal triggers in writing this article is another belief. The retirement industry must join the race to provide next generation technology to savers before it's too late, for the sake of the industry itself.

While banks, and other service providers offer true '21st century' technology to their users, pensions and retirement plans often leave members underserved in the most crucial area of their financial lives: the savings they've put aside for their entire working life to serve their future.

At Smart, we've quickly become the leader in this space, and I want to share some thoughts on why the industry is where it is, and how we've reached the position we have.

A WIDENING TECHNOLOGY GAP: STRUCTURAL ISSUES LIMITING TECH IN THE RETIREMENT INDUSTRY

In real terms, there has been great difficulty among the industry's incumbent providers to move quickly to address a widening technology gap. The investment required has always looked large, 'technology' is not a core competency of most sizeable retirement savings providers, and naturally there's always trepidation when it comes to spending money in areas where the status quo is seen as preferable in comparison to the perceived risk.

And, it may be a cliché, but we all know about skating to where the puck is going, rather than to where it is or it has been. The 'moving target' of digital change has in some cases proven a barrier to change and served to widen that gap.

However, the broader picture is that this is a challenge that isn't insurmountable. If we look at the benefits that technological innovation has brought to other financial markets, we can see them as incentives. They represent the opportunities in our own marketplace, for providers and consumers alike, for creating value, streamlining efficiencies, increasing competitive advantage and driving better outcomes.

In framing the issue, perhaps what's been missing is the long-term view. Whilst investment in technology may have brought more immediate benefits and returns more quickly in other markets, the difference is that retirement savings – a pension plan – is by nature a long-term product. It follows that when it comes to pensions, for both consumers and providers there's therefore always going to be a perceived 'oil tanker effect' – the problem that you can't always immediately see the consequences of the decisions you make.

However, the sheer size of the international pension market means that there's a compelling case for technological investment. While the average bank savings account may hold a few thousand at any point, a single retirement savings account may reach hundreds of thousands, or beyond.

A UNIQUE SET OF HURDLES

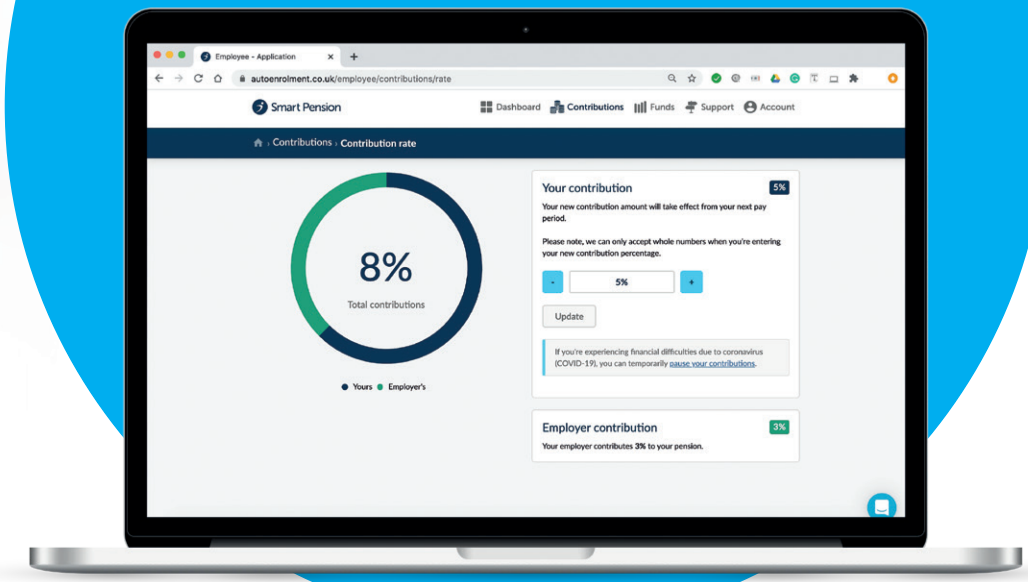
We've talked about the incumbent players a little. But why has the retirement market been so overlooked by the startup ecosystem? With a $47trillion (and growing) 'total addressable market', surely it's the perfect opportunity for venture capital?

The answer is in a unique set of hurdles. Investors are keen to place big bets in this area, but have found themselves hampered by a lack of viable startups and scaleups possessing the three key pillars to disrupt this market for the better:

1. Ability to penetrate an apparently opaque market
2. An opportunity that's provable in a short enough timespan
3. Technological excellence offering a true user benefit

Maybe what has held the investment in transforming the pension business back to date is a unique set of hurdles. After all, it's a market in which the barriers to entry are quite high, in that it requires a high level of existing and specialist knowledge, an opportunity above and beyond the norm, and an organisation with a fairly unique set of skills.

Perception problems could also inhibit change. If we think of tech entrepreneurs, we think of people in their 20s and 30s, a young demographic and therefore one with less experience of the pension business. With less exposure to the industry, there is a lower ability to



Employee - Application

autoenrolment.co.uk/employee/contributions/rate

Your contribution 5%

Your new contribution amount will take effect from your next pay period.

Please note, we can only accept whole numbers when you're entering your new contribution percentage.

- 5% +

Update

If you're experiencing financial difficulties due to coronavirus (COVID-19), you can temporarily pause your contributions.

Employer contribution 3%

Your employer contributes 3% to your pension.

understand the key drivers within the market, and the opportunities to benefit 'end users'. At Smart, our mission is to transform pensions, savings and financial well-being, across all generations, around the world. With our unique experience across technology and finance, and that guiding mission, we placed ourselves in the position to transform the areas that count for the better.

While retirement savings is an industry that has the potential to impact the entire world for the better, it's a shame that for some the perception is essentially a business that's seen as 'out of touch'. In a world where delayed gratification is far from the norm, the contrary 'pay now, buy later' proposition may make a pension plan a much tougher sell, despite its huge importance.

A LEGISLATIVE BARRIER AND A LEGISLATIVE OPPORTUNITY

Fear of legislative change is another factor holding back the retirement tech market: Some fear the products they build may quickly be made irrelevant, in an area where legislative change is common. At Smart we see this as a huge opportunity area, rather than an area of risk. With legislative change comes opportunity, and we're now at the stage where we've built our technology platform to the extent that it can adapt with legislative change.

In fact, though it may sound strange to those more used to the broader fintech world, our platform is now mature enough that it can enable legislative change should governments wish to use it for such a purpose. A government may ask: 'How can we put 'opt in by default' retirement saving legislation in place, when there are no providers to support it?' – whereas in the past a government may see this as such a blocker that they don't see it as a possibility, our platform can enable it in months. It may be used by large financial providers, already in the market, to meet those requirements, and can be tailored to match legislative nuance.

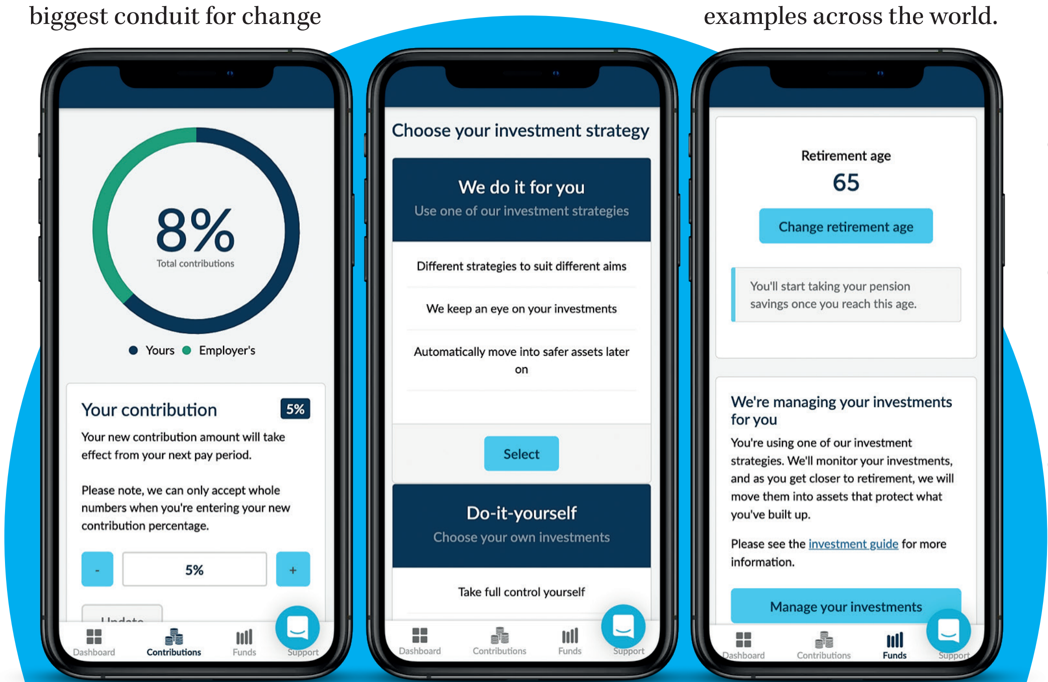
Indeed, in our experience, the biggest conduit for change in the pension industry hasn't come from within the industry itself. Instead, it has come in the form of regulatory change.

As an example, in the UK, the introduction of 'auto enrolment' – the idea that every working person should be automatically opted in to a pension scheme unless they specifically choose to opt out – created a testbed; a favourable and incentivised environment that didn't previously exist. From our own perspective, that offered the opportunity for us to create technology to better serve the UK population. Regulatory change was indeed the driver to how Smart's business started.

Importantly, at the same time as the introduction of this 'stick' from the government, in more general terms there was a carrot of sorts, too. Technological change meant that consumers had confidence in financial technology for retirement savings as a whole and were comfortable using it. That added up to make good news not only for us but also for the industry as a whole and, perhaps most importantly, the consumer.

A WORLDWIDE PROBLEM BUT AN INTERNATIONAL OPPORTUNITY

Taking a global view, regulatory change continues to be an important factor, accelerating the need for innovation in our industry. At Smart, we see similar examples across the world.



Your contribution 5%

Your new contribution amount will take effect from your next pay period.

Please note, we can only accept whole numbers when you're entering your new contribution percentage.

- 5% +

Choose your investment strategy

We do it for you
Use one of our investment strategies

Different strategies to suit different aims

We keep an eye on your investments

Automatically move into safer assets later on

Select

Do-it-yourself
Choose your own investments

Take full control yourself

Retirement age
65

Change retirement age

You'll start taking your pension savings once you reach this age.

We're managing your investments for you

You're using one of our investment strategies. We'll monitor your investments, and as you get closer to retirement, we will move them into assets that protect what you've built up.

Please see the investment guide for more information.

Manage your investments

As populations age, and governments look ahead to the future, more are looking at options to ensure the financial wellbeing of their people. This is true when we look at Europe, Australia, or the Middle East, or the USA – where the 'SECURE Act' spells out the need for 'Setting Every Community Up for Retirement Enhancement'. Changing societal needs have created an opportunity and this in turn has forced regulatory changes, and schemes globally have had to evolve with this. With the rapidly changing behaviours in people's everyday lives, people expect exactly the solutions that have the potential to improve their lives.

THE IMPACT OF THE COVID-19 PANDEMIC

The technology gap in the pensions and retirement industry has come into sharp focus and is especially relevant now, due to the effects of the Coronavirus pandemic across the world. It has prompted many to pay much closer attention to their retirement income. At Smart, we constantly look at factors within the retirement market, globally, in particular to monitor evolving user needs. In a recent survey we carried out of 6,000 people across three continents, we found the nature of retirement is changing and fast.

- In the UK there is an increasing desire to manage retirement saving and spending without any outside assistance. That would be great, were it not for a lack of solutions to help them understand their position and make decisions
- One in eight adults (13 per cent) over the age of 55 are planning on delaying their retirement due to the Covid-19 pandemic
- In Australia, where the pensions and retirements industry is among the most mature in the world, there is still a gap in knowledge – one third of respondents simply did not understand the retirement finance options available to them
- And, in the US, where those asked wanted to manage their retirement finances themselves, 21 per cent of respondents – one in every five people explicitly wishing to manage their own options – did not understand all of the options available to them

Technology has the opportunity to help here – guiding savers on their best paths forward. But a lack of great, flexible, user-centric technology in the area robs many of an informed ability to plan. Similar insights fuelled our will to build 'Smart Retire', to solve such problems, a global first in an area where there is enormous demand.

At the same time as those reaching retirement are looking for solutions, the fallout of Covid-19 may mean a mixed picture in terms of wider investment in the area. For the wider market beyond our own technology, it is potentially a very delicate balancing act. Specialisation and sustainability, along with long-term profitability, are going to be key. To counter this 'gap', we are keenly investing further to benefit end savers across the world and offering partnership opportunities with our platform.

IN SUMMARY

At a time when retirement savings are more important than ever, there is a dearth of attention on innovation in this area.

At Smart, we recognised this and, taking a legislative change as an opportunity, we used our 'clean sheet of paper' ethos to building technology, and a great focus on user research to deliver actual benefits to savers before it's too late. Our platform allows financial organisations and governments across the world to take advantage of 21st century tech to address this.

The retirement savings world is at different stages of maturity across the globe, but, just as fintech has solved many of the world's greatest issues in recent years, in each region there are opportunities to bring benefits to retirement savers – and those during retirement – through great technology. TFT

About Smart

Smart is a global technology business that focuses on modernising and innovating in the pensions and retirement savings industry – a sector now worth nearly $50trillion globally and growing at eight per cent a year. Our Smart Platform is revolutionising saving for and spending in retirement, supporting both business and members towards better outcomes and financial wellbeing. As well as our platform, our technology powers our UK-based master trust scheme, helping hundreds of thousands of members save for retirement. We have a clean sheet of paper, always looking at things with a fresh perspective, and not just doing things a certain way because that's the way it's always been done.

Website: www.smart.co

Linkedin: linkedin.com/company/smart-pension

Twitter: @smartpensionuk

Smart

Cybersecurity in the Middle East and Africa

Rapid digitalisation in the MEA region has resulted in a burgeoning market for security solutions

Richie Santosdiaz, Head of Middle East and Africa (MEA), *The Fintech Times*

As Middle East nations strive ahead in the adoption of new technologies, and governments in the region increase investments in digital transformation, cyber threats are also dramatically expanding while becoming more complex.

According to a report from Mordor Intelligence, the cybersecurity market in MEA was valued at $7.174billion in 2019 and forecast to register a compound annual growth rate (CAGR) of 14.08 per cent during 2020 to 2025.

Another report from ResearchAndMarkets.com suggests the same. For its pre-Covid-19 forecast, the Middle East cybersecurity market was projected to grow from $16.1billion in 2020 to $28.7billion by 2025 with a CAGR of 12.2 per cent. Interestingly, its post-Covid-19 forecast increased that – its CAGR rate now looks to be at 13.8 per cent with a 2020 figure of $15.6billion to a 2025 forecast of $29.9billion.

There are various other reasons why it plays a large role in the MEA region but at the end of the day, it is generally the region's rise in digital transformation in a short period of time. At top level, much of the region has been undergoing various economic development strategies.

For instance, in the Gulf Cooperation Council (GCC) region, all of the six GCC members have their own variants of their wider strategies of some sort (Bahrain Economic Vision 2030, Kuwait Vision 2035, Qatar National Vision 2030, Oman Vision 2040 and Saudi Vision 2030).

The United Arab Emirates (UAE), for instance, not only has other national initiatives, such as UAE Centennial 2071 and UAE Vision 2021, but also variants in respective Emirates, such as Abu Dhabi Vision 2030. In addition, other initiatives in Saudi Arabia, part of its wider 2030 strategy, also include a new artificial intelligence (AI) strategy that will help propel the Kingdom to be a leader in that area.

As much of the wider economic development diversification has prioritised digital transformation, countries, such as the UAE, have become leaders in digital transformation. In other parts of MEA, such as in Africa, digital transformation either has come as part of its large national economic strategies – like Egypt – as well as other governmental support initiatives, whether they include being part of an economic development strategy or not. In the fintech space, highlights in Africa were felt across much of the continent – from Nigeria to South Africa to Angola to Ghana to Kenya – to name a few.

They included announcements from planned fintech strategies to fintech offices. Israel, known as a 'Startup Nation,' is also a global leader in cybersecurity. Israeli startups received $1.19billion (almost 20 per cent) of global VC investments in cybersecurity, according to the *Israel's Cybersecurity Industry from Start-up Nation Central Report.*

The same report highlighted that there are around 450 cybersecurity companies operating in Israel. The country has had an industry since the 1980s, where companies began developing anti-virus software and information security.

They have been at the forefront for much of wider tech innovations and particularly in cyber, such as the Israeli Ministry of Finance's fintech-cyber innovation lab programme, the first initiative in the world that leverages governmental assets and data in order to promote fintech and cyber startups in an open innovation platform.

Examples of Israeli cyber companies include Imperva, Check Point, Radware and CyberArk – to name a few. The country, with its tech scene and history of cyberattacks, coupled with other factors, such as promoting the sector and educating the youth on tech in general, shows much of the innovationits cyber industry has produced on a global stage.

On another note, in Turkey, the country is now ranked 20th on the Global Cyber Security Index as a result of the country's efforts to strengthen its sovereignty in the cyber domain, led by the country's Vice President, Fuat Oktay.

Even before Covid-19, fintech played a large role and during the pandemic and beyond most likely will continue to do so. This includes the likes of contactless payments and other mechanisms where consumers and companies are providing sensitive data, which exposes people to potential cyberattacks. For instance, as in MEA as a whole, where over one in nine point of sale (POS) transactions are now contactless and also the growth of online shopping as well can expose more potential challenges.

> MEA will continue to see an importance in cybersecurity due to its growth in digital and wider digital transformation – even before the 2020 pandemic that made much of us go virtual and digital

The Morder Intelligence report highlighted examples, such as in the UAE. Smartworld stands to be the first cybersecurity centre that will provide continuous monitoring of online threats and cyber threat management to companies across the region's government and private sectors. One company – Tata Communications – has unveiled an advanced cybersecurity response centre in Dubai.

In terms of Africa, the growth of non-cash volume due to the continent's young population will grow the demand for cybersecurity. The same report says: "This factor is expected to drive the new mobile money and digital payment schemes, with Kenya emerging as regional leader in the implementation and uptake of mobile payment solutions, such as M-Pesa. Augmenting this trend, ABK Egypt, with 39 branches and 85 ATMs across the country, has employed Cisco's cybersecurity solution to stay at par with the country's digital transformation."

Despite research showing an overall decrease in certain malware families and types in sub-Saharan Africa in H1 2020 (36 per cent decrease in South Africa, 26 per cent decrease in Kenya and a 2.7 per cent decrease in Nigeria), Kaspersky research has warned that the human cyber threat remains rife.

Africa is not immune to the evolving techniques of advanced persistent threats (APTs), as well as the possibilities of being a future target of hacking-for-hire threat actor groups. In the Middle East, the GCC, which pre and during Covid has seen banks accelerate their digital transformation, cybersecurity to protect their customers' accounts and investments will also continue to grow.

Finally, beyond just fintech but in our day to day lives, the demand for cybersecurity in the region has gained traction in the water systems and pumping stations due to automation, where the threat of cyberattacks has increased in the region. MEA will continue to see an importance in cybersecurity due to its growth in digital and wider digital transformation – even before the 2020 pandemic that made much of us go virtual and digital. TFT

TACKLING ONLINE THREATS IN THE US

US fintechs are trying to outflank cyberattackers, who are looking to make hay amid the coronavirus crisis

John Reynolds, Journalist, *The Fintech Times*

Millions of US citizens are subject to cyberattacks each year, as nefarious actors look to outwit individuals, businesses, healthcare and educational institutions, as well as government bodies.

Phishing, denial-of-server, malware, password attacks, intellectual property theft, rogue foreign attacks and espionage are among the cyber threats these institutions are looking to detect and deter, as criminals become ever more sophisticated.

Challenger banks – and other fintechs – are prime targets for rogue operators, as victims of cybercrime can be carrying out something as innocuous as online shopping or online banking.

Meanwhile, the target on the back of fintechs, in the eyes of criminals, is growing even bigger courtesy of high-profile funding rounds and M&A activity.

A boss at a US fintech trade body underscored how important having top-notch cybersecurity is to fintechs.

"For any bank or fintech, that holds account numbers, the customer's money, or both, cybersecurity is of paramount importance, protecting these assets is key," says Scott Talbott senior vice president of government relations at the Electronic Transactions Association (ETA). "Your business depends on it, your reputation depends upon it."

Talbott adds that cybercriminals are always trying to get ahead of fintechs.

"We build a 10-foot. wall, they [hackers] build an 11-foot ladder. So, we need to build a 12-foot wall. We can never rest and we must always be vigilant in terms of cybersecurity."

Failing to detect and deal with a cyberattack can ruin a fintech's reputation. Meanwhile, coronavirus has upped the risks of cybercrime and financial fraud, as hackers attempt to capitalise on fears about coronavirus and the fact many people are working from home.

RECENT EXAMPLES OF CYBERATTACKS

A cyberattack, it seems, is seldom out of the headlines. Most recently, a massive trove of US government emails were targeted in a hack understood to be carried out by Russia, according to US officials.

The hack – the biggest against US officials in years – started when a pernicious code was sneaked into updates to the popular software called Orion, made by SolarWinds, which monitors the computer networks of businesses and government for outages.

Despite the mayhem wrought by the hack, high-profile data breaches like SolarWinds help keep cybersecurity in the public conscious, potentially making the public minded to be careful, according to John Mileham, CTO of Betterment, the New York-based digital wealth company.

CYBERATTACKS RESONATE IN PUBLIC CONSCIOUSNESS

Mileham comments: "Cybersecurity is very front of mind for folks given the recent SolarWinds breach. There is a growing awareness of cyber threats as a thing in people's minds as more data breaches have happened and as various high-profile hacks have taken place."

Fintechs have not been immune to recent cyber hacks. Last year, Robinhood, the California-based trading app, had 2,000 trading accounts hacked, according to Bloomberg. In response, Robinhood said a 'limited number' of accounts had been compromised and also sent a push notifications through its app encouraging its users to implement a two-factor authentication.

MAJOR CYBER THREATS FACING TODAY'S US FINTECHS

So, what are the top cyber threats facing today's US fintechs? Criminals wanting to make money are the top of the tree for Betterment, according to Mileham.

He comments: "We find that our primary threats are and remain criminals. And, they are operating with a business model that only allows them to spend so much time and energy compromising a given institution or compromising an individual customer within an institution in order to turn a profit."

Fending off customer fraud ranks top on investment app Stash's list. Gavin Grisamore, VP of information security at Stash, said: "Mitigating any threats of customer fraud or account takeovers are the top priority for Stash's cybersecurity team. Maintaining customer trust is absolutely vital."

Distributed denial-of-service (DDoS) attacks – where hackers try and make a website or computer unavailable by flooding or crashing the website with too much traffic – are becoming more commonplace, says Steven Gall, VP of engineering at M1 Finance, the Chicago-based money management platform.

"We have never had a data breach," says Gall. "But we are always under attack. It's naïve to think you are not."

IMPACT OF COVID-19 ON CYBER THREATS

Firms and government agencies have warned consumers of increased risks of cybercrime and financial fraud amid coronavirus, as hackers attempt to capitalise on fears about Covid-19 and the fact that so many people are working from home, often logging onto new virtual computer systems.

"So, coronavirus definitely changed the cyber threat landscape a bit. There was a massive uptick in unemployment insurance fraud in the US, "said Mileham.

"This required us and our partners to work together to help get our arms around it, make sure that we were able to serve our customers without putting them at undue risk."

Gall says at M1 Finance, it has invested heavily in ensuring its cybersecurity policy is enforced amid a workforce working remotely, so it's able to carry out measures like auditing staff workstations remotely.

Gall points out that many data breaches occur when temporary users are granted god-like powers across systems in firms, that are never viewed and audited.

He stresses the importance of ensuring staff are only given the online privileges their jobs require, never more.

TIE-UPS WITH PARTNERS CAN HELP WARD OFF A CYBER THREAT

US challenger banks' partnerships with existing banks can help shore up their handling of a cyberattack, suggests Talbott.

"When a challenger banks or an internet bank works with an existing bank, that existing bank is going to make sure that the challenger bank is compliant with all the laws and regulation that the traditional bank is subject to," he says.

Grisamore says that Stash "works with several key organisations across sectors to ensure the company is up-to-date on the latest cybersecurity intelligence and trends".

Meanwhile, Mileham argues that its proprietary technology gives it an advantage to other financial institutions in combating the cyber threat challenge.

Betterment has "built and maintains its own technology" which "allows us to provide better consumer service while tailoring specifically to the risks and threats we face as a business".

"It allows us to be more responsive to new threats. It allows us to build next generation solutions to cybersecurity challenges and roll them out quicker than you would be able if you were working heavily with vendors and vendors of vendors."

Gall gives an example of a company M1 Finance works with, which recently told its customers it had been subject to 'unauthorised access' of its systems, but was not sure if its customers' passwords had been compromised. Gall says it's 'alarming' and 'concerning' that the company was unable to disclose specific deals about the access, pointing out that M1 Finance's own systems would have handled the situation better.

SIZE OF FINTECH CYBER TEAMS

At Betterment, Mileham says it has an overall team of around 100 engineers which builds the Betterment product, within which sits a 'small' cybersecurity team that has four dedicated engineers focusing on security.

Mileham adds: "They work in partnership with engineers who build the product to help secure it through a variety of means."

This includes carrying out exercises like penetration tests and simulating events like data breaches. Likewise, M1 Finance has a small dedicated team of three concentrating on implementing security but Gall says the key is having a 'security-focused organisation'. Stash, meanwhile, has a team of five full-time cybersecurity engineers.

"The team is primarily tasked with detecting any potential threats to our customers and the businesses at large," says Grisamore. "They're also in charge of assessing Stash's technology footprint across the internet and reducing its attack surface to the greatest possible extent." TFT

HELPING HAND

__Nicolai Solling__, CTO of __Help AG__, talks about the importance of cybersecurity in the ever-evolving world of fintech

Help AG, the cybersecurity arm of Etisalat Digital, provides enterprise businesses across the Middle East with strategic consultancy combined with tailored information security solutions and services to help them evolve securely with a competitive edge. Headquartered in the United Arab Emirates, Help AG has been present in the Middle East since 2004 and has established itself as one of the region's most trusted advisors.

Nicolai Solling has worked in the IT and network industry for more than 20 years. In his role as chief technology officer of Help AG, he is responsible for overseeing the company's professional services, support services and technical vendor management across the region. Since joining the company in 2008, he has successfully grown the technical team by more than 200 per cent and has been heavily involved in the design, deployment and operation of some of the most challenging network and security infrastructures for enterprise customers across a variety of industry sectors.

The Fintech Times caught up with Solling to discuss the danger of increasingly sophisticated cyber threats.

THE FINTECH TIMES: What has been the traditional Help AG response to helping secure the latest financial technology innovations?

NICOLAI SOLLING: The financial sector has always been a major focus area for Help AG due to the risk-averse nature of financial organisations and the specific requirements they need to have fulfilled to ensure their security, especially in light of digital transformation. Help AG recognises the critical importance of securing the huge amounts of sensitive data that go into fintech as organisations in the financial sector face a higher risk of experiencing a cyberattack.

Traditionally, Help AG has offered services, such as penetration testing, red teaming, endpoint security assessment, managed detection and response etc, to protect fintech innovations. We have been an early advocator of email security and have focused on implementing application security and enabling a secure cloud journey for financial organisations looking into utilising public and private clouds and cloud compute technologies, such as container-based services and micro-based services.

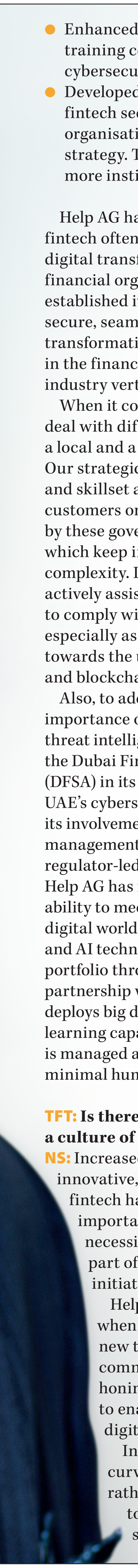
Help AG has also established strong partnerships with reputable vendors to offer valuable technologies that further boost the security posture of financial organisations, such as Palo Alto Networks' cloud security capabilities, F5's application firewalls, ShiftLeft's focus on securing the application code, and Aviatrix's solutions that emphasise creating a secure network fabric for your cloud environment whether it is on-prem or the public cloud.

By having rightly skilled talent and continuously broadening its capabilities, Help AG is able to articulate the value of these technologies and offer them within the market successfully. One of our major success cases within the financial industry is our involvement in the creation and implementation of Dubai Financial Services Authority's (DFSA) managed threat intelligence platform (TIP) which enables it to advise its members in a timely manner in case of a malicious activity.

TFT: How has your support changed over the past few years?

NS: Help AG has recognised the rising importance of financial technology in business and has accordingly:

- Bolstered fintech security offerings by partnering with world-class vendors, including Proofpoint, which offers solutions that help protect applications and manage email threats like business email compromise (BEC)



- Enhanced expertise by training consultants on fintech cybersecurity applications
- Developed expertise in integrating fintech security as part of an organisation's enterprise security strategy. This is important as more and more institutions adopt fintech

Help AG has also recognised the role fintech often plays in organisations' digital transformation, particularly financial organisations, and has established itself as a key enabler of secure, seamless and effective digital transformation for its customers, both in the financial sector and across other industry verticals.

When it comes to data privacy, banks deal with different types of regulations on a local and a global scale, such as GDPR. Our strategic consulting team's expertise and skillset allows them to guide customers on how they are impacted by these governance frameworks which keep increasing in number and complexity. It also enables them to actively assist financial organisations to comply with regulatory frameworks, especially as they move increasingly towards the usage of cryptocurrencies and blockchain technologies.

Also, to address the increasing importance of accessible, actionable threat intelligence, Help AG has assisted the Dubai Financial Services Authority (DFSA) in its initiative to support the UAE's cybersecurity strategy through its involvement in the creation and management of the first financial regulator-led managed TIP in the region. Help AG has further strengthened its ability to meet customer needs in today's digital world by incorporating automation and AI technologies into its comprehensive portfolio through entering into a strategic partnership with SECURITI.ai, which deploys big data analytics and machine learning capabilities to ensure data is managed and cleared securely with minimal human intervention.

TFT: Is there anything that has created a culture of change inside Help AG?
NS: Increased awareness of the innovative, ever-evolving nature of fintech has only reinforced the importance of cybersecurity and the necessity of treating it as an integral part of every digital transformation initiative taken by organisations.

Help AG has been a pioneer when it comes to introducing new technologies and is committed to upgrading and honing its customers' capabilities to enable their secure digital transformation.

In addition, to stay ahead of the curve, Help AG takes a predictive rather than a reactive approach to market conditions. This specifically enhances our hiring process as it impacts the skillset we look for in cybersecurity talent. For example, we have been increasingly hiring experts with skills in DevOps and microservices security architecture.

Another notable aspect that has been contributing to creating a culture of change is Help AG's service centric business evolution, which makes sure we understand customers' needs better and provide them with tailored services that have the required technology embedded.

TFT: What fintech ideas have been implemented in Help AG?
NS: Help AG utilises digital transformation capabilities not only for its customers but also for its business, using private and public cloud while aiming to limit the footprint of its on-prem data centre by migrating services into the cloud and implementing the right security controls to ensure their safety. Moreover, Help AG's pen testing team is constantly assessing fintech and e-commerce applications to ensure organisations stay safe.

> Digital transformation has increased agility and scalability for Help AG. By using the power of cloud and automation, we have been able to scale up significantly without needing to increase backend personnel. This has brought in increased efficiencies, which ultimately facilitates sustainable growth

TFT: What benefits have these brought?
NS: Digital transformation has increased agility and scalability for Help AG. By using the power of cloud and automation, we have been able to scale up significantly without needing to increase backend personnel. This has brought in increased efficiencies, which ultimately facilitates sustainable growth.

TFT: Do you see any other industry challenges on the horizon?
NS: A possible increase in ransomware attacks is anticipated. Ransomware that targets user devices and clouds can threaten infrastructure, resulting in significant insurance losses. Our research has also uncovered a significant increase in carding, the illegal usage of a credit or debit card by unauthorised individuals to buy a product. Help AG found a 500 per cent jump in risk alerts for carding between 2019 and 2020.

Furthermore, the evolution of consumer needs has led to new digital habits, hence leading to an increase in e-commerce and application development. Cybersecurity needs to keep pace with the increase in e-commerce; rapid digitisation in commerce brings concerns regarding authentication, the security of sensitive data, etc. Help AG is a frontrunner in ensuring security is a day-zero consideration while new applications are developed and released for large scale usage.

In addition, Covid-19 has accelerated the pace of cloud adoption and digital transformation like never before. This introduces cybersecurity challenges that require fundamental shifts in an organisation's security approach. With our secure cloud enablement strategy and continuing focus on security automation, we are empowering a secure transformation journey for enterprises and governments. To further secure digitalisation efforts, we launched our Help AG secure private access (HPA) service – a scalable and locally delivered zero trust network access (ZTNA) service providing businesses with holistic security, visibility and control across environments.

Impending industry challenges also include an increase in distributed denial of service (DDoS) attacks. Our research has revealed that the region has been witnessing a tremendous growth in DDoS attacks – in frequency, volume, new attack vectors and multifaceted tactics. This growth is expected to increase as people worldwide continue working remotely, relying on VPNs, and using unsecure networks and devices. To safeguard its clients, Help AG operates a round-the-clock managed DDoS protection service, which offers volumetric and application layer attack protection and deep traffic visibility and reporting.

The other challenges that the industry will have to brace for include increases in phishing, data breaches, third-party security risks, application security risks, and the usage of unsecure electronic gadgets and internet of things (IoT) devices to conduct transactions. Consequently, the regulation of the fintech industry and financial entities is bound to increase, which will lead to changes in financial services and how we deal with their providers.

TFT: Can these challenges be aided by fintech?
NS: Digital transformation is changing risks, as theft turns from being physical to digital. However, blockchain technology enables all digital transactions to be traced which serves as an advantage against cybercriminals. Blockchain may also be useful in warding off ransomware attacks.

Some fintech applications can help increase data security, lessening the chances of card information being leaked or stolen, while other fintech applications can help increase cybersecurity in e-commerce, e.g. digital identities.

AI-driven fintech is critical in ensuring compliance with the GDPR framework, which protects the customer's data and supports their right to be forgotten, by ensuring data privacy through automated processes with the least human intervention possible. This is where our partnership with SECURITI.ai plays a vital role, providing data protection through automation.

TFT: What else can we expect from Help AG?
NS: Fintech is an innovative, thriving industry that will only become more and more important with time, whether for financial institutions like banks or institutions in other sectors. It is crucial that cybersecurity is tightly integrated into every step of fintech innovation to secure sensitive data and transactions and avoid incurring financial losses. Without dynamic cybersecurity solutions, organisations that utilise fintech will put themselves at risk of cyberattack, possibly resulting in reputational damage, business disruption, and fraud.

Help AG is the biggest cybersecurity service provider in the region, with an experience that spans more than 25 years. Powered by Etisalat, we are enviably positioned as the strongest force in the field of digital security – in terms of the number of qualified experts, digital domain expertise and financial flexibility. TFT

AT A GLANCE

WHO WE ARE: Help AG provides leading enterprise businesses across the Middle East with strategic consultancy combined with tailored information security solutions and services that address their diverse requirements, enabling them to evolve securely with a competitive edge. Founded in Germany in 1995, we have been present in the Middle East since 2004 and we implement security solutions for the customer from A to Z.

COMPANY: HelpAG
FOUNDED: 1995
CATEGORY: IT & digital security services
KEY PERSONNEL: Stephan Berner, CEO
HEAD OFFICE: Dubai, UAE
ACTIVE IN: UAE, Gulf Cooperation Council and the Middle East
WEBSITE: www.helpag.com
LINKEDIN: linkedin.com/company/help-ag
TWITTER: @HelpAG_ME

Social value – at the tap of an app

It's time to open up open banking, says payments specialist ***allpay***

To kick-start 2021, fintech needs its 'Rashford moment' – the point at which (social) problem solving is a how-to lesson for the UK government from those that have 'been there' and are willing to 'go there'.

For Tony Killeen, the owner and managing director of allpay – a provider of complete payments services, including credit cards, pre-paid cards, direct debit and bill payment collection – that means opening up open banking. Specifically, the adoption of bill payment solutions – an initiative borne out by allpay's research as the pandemic pitches household finances over the brink.

"If fintech is to prove its worth beyond Covid, innovate to accumulate must account for inclusion as the fallout from the pandemic pushes the prospect of a cashless society ever closer," says Killeen.

The way, then, to make social value pay.

As Covid-19's first wave engulfed the UK, an allpay survey exposed the extent to which fintech can shift the pre-pandemic payments landscape.

The survey findings were released with the sector working to a stark pre-pandemic assessment of financial exclusion in the UK. An estimated 1.3 million adults lacked a bank account with 3.1 million having one or more high-cost loans charging more than high street banks.

"It's too easy, if not dismissive, to set those effectively paying what amounts to a poverty premium against the estimated 97 per cent of UK adults holding an account they can use to make day-to-day payments and transaction – a current account in around 96 per cent of cases. To this end, open banking becomes both the question and the answer," said Killeen.

The allpay UK-wide survey took in a 2,000 strong sample as insight into payment methods for household bills over 2019 to 2020. Those pre-pandemic bill payers were still invested in cash, with cash office payments taking preference over options, such as PayPoint, Post Office and Payzone.

The stats also acknowledged an ongoing decline in direct debit use as cash remained a key focal method with a steady rise in bank transfer, credit card and standing order payments over the past three years. Monthly payments were the most popular frequency in all household bills, although the stats show payees have increased their preference in quarterly and four-weekly payments – quarterly instalments for rent (61 per cent) and council tax (50 per cent) significantly increased year-on-year.

Mary Cotton, allpay's head of operations, said the continual reliance on cash – as shown in the survey – was shared among a significant number of payees – to the extent that it represented an average of seven per cent for each bill payment.

"With many businesses moving towards a cashless society, the stubborn rate at which the method remains showcases its value to many in the UK payments space. This year's results demonstrated that 13.5 per cent of rent payments alone were made utilising cash, with more than 75 per cent of these made at business offices – often cited as a cost-intensive source," said Cotton.

But the survey findings also exposed reduced consumer confidence in paying household bills, with fewer fully confident in managing money to the extent of a year-on-year decline of two per cent to just 78 per cent. Just this month, the Resolution Foundation thinktank released a report revealing more than a third of the UK's poorest families spend more on food, gas and electricity – after years of weak growth in living standards.

The allpay respondents referenced 'ease of use' as the most common reason when choosing their payment method and nearly 1,000 respondents said that reminders via text or email would make paying their household bills easier, with the stats showing direct debit is still the most popular payment type across all household bills,

For fintech, the allpay findings add up to opportunity inherent in the green paper the government slipped out between Christmas and New Year outlining intentions toward the 'transformation' of public sector procurement

ALLPAY/TLF CONSUMER SURVEY 2019-20 KEY FINDINGS

- Credit cards, standing orders and bank transfers provided the three largest increases across 2018-2020
- Cash payments remained static across the **three** years – representing seven per cent average across each bill
- Debit Card usage increased slightly across the **three** years – albeit a small decline y-o-y (2019-2020)

  – Notable three-year increase in mortgage payments
- Credit card usage has increased the most out of all channels

  – **2%** on average across each bill from 2018-2020

  – Direct debit is most popular for the third year running – although averages fell by **5%** each bill

  – Rent and insurance payments lost **15%** and **10%** market share across the three years

  – Direct debit take-up is highest among electricity, gas and internet/phone – with more than **60%** of respondents opting for the channel

  – Rent has the lowest direct debit take up across all household bills – standing at **26.5%** with a loss of nearly **15%** market share over three years

  – Next lowest share sits with insurance at **47.5%**

  – Bank transfer, cash, cheque and credit cards all increased their average market share year-on-year

  – Credit card usage increased by nearly **49%** y-o-y for council tax payments

  – Company offices to make cash payments increased across all household bills
- A **46%** year-on-year increase for rent – with only **24%** making payments at PayPoint, Post Office and Payzone
- Respondents referencing 'ease of use' as the most common reason when choosing their payment method
- **998 respondents** said that reminders via text or email would make paying their household bills easier
- The usage of PayPoint, Post Office and Payzone declined across every household bill – with cash office payments taking preference
- **76%** of cash payments for rent taking place at cash offices

  – More than **50%** of council tax payments remain at PayPoint, Post Office and Payzone outlets – a **7%** decrease over the past three years

  – Paying online continues to be the most favourable method for those paying by debit card – with the usage of mobile apps increasing rapidly

  – Mobile app usage for debit card payments has increased significantly across water bill (**33%**), rent (**100%**), mortgage (**90%**), council tax (**58%**), TV Licence (**46%**), insurance (**45%**), and internet/phone (**72%**)

  – A significant decline in the set-ups of direct debits – reflected in the decrease of overall respondents utilising the payment method across each of the household bills

  – Set-ups of bank transfers has considerably increased, reflected in the sharp rise in bank transfer payments for all household bills

with an average take-up of 55 per cent, though usage decreased by five per cent across three years.

Rent payments registered the lowest share against all other bills (26 per cent), with the most popular across internet and phone (70 per cent) and electricity and gas (61 per cent) bills. Debit card payments were the second most popular payment method, despite showing a small decline (five per cent) on average per bill from last year.

Take up for the second consecutive year is highest in both rent and insurance payments, with the use of credit cards the largest increase of all payment methods across the three years (2.2 per cent).

Monthly payments continue to be the most popular frequency in all household bills, although payees have increased their preference in quarterly and four-weekly payments. Quarterly instalments for rent (61 per cent) and council tax (50 per cent) significantly increased year-on-year.

For fintech, the allpay findings add up to opportunity inherent in the green paper the government slipped out between Christmas and New Year outlining intentions toward the 'transformation' of public sector procurement.

Essential to this transformation are measures encouraging awards to a more diverse range of suppliers pitching to contract terms and tender evaluations intended to take a broad view of value for money – with an emphasis on social value. This includes award criteria for evaluating final bids and scoring their quality, to encourage ways of working and operational delivery that achieve social value objectives.

As advanced by the government, this approach allows buyers to include criteria that go beyond the subject matter of the contract and encourage suppliers to operate in a way that contributes to 'economic, social and environmental outcomes based on the most advantageous tender'.

allpay has recently teamed up with the NHS and other partners to transform the national Healthy Start scheme, with digitisation pitched as making the scheme simpler to access, easier and more flexible to use in replacing the present paper-based voucher scheme from February this year.

This transformation is expected to incrementally increase the support of the Healthy Start scheme from 300,000 beneficiaries a year to circa 500,000 a year once fully transitioned to a digital solution – with the potential for up to 750,000 individual applicant accounts to be created throughout its full term.

allpay will use its prepaid solution to facilitate top-ups to the scheme's new payment cards, enabling funds to be spent on the likes of fresh milk, fresh or frozen plain fruit and vegetables and infant formula, in all major supermarkets, many local shops and markets. And, allpay has already seen how this can work with the success of its solution for the Scottish government as it shifted its stance on food poverty – a solution saluted as Social Inclusion Project of the Year at the 2020 Payments Awards.

The allpay initiative enabled Scotland to disburse vital funds to low-income households while retaining full autonomy over those funds – managing the scheme through a streamlined, automated process supported by advanced analytical tools to use. Named Best Start Foods, the prepaid card programme allowed for the purchase of 'healthy' products from retailers free of the requirement to register that came with the previous voucher scheme – with the card accepted in any grocery store displaying the Mastercard logo.

To date, around 39,600 cards have been issued to those eligible for the scheme with a total load value closing in on £10million. Some 697,646 transactions have occurred since the scheme went live in August 2019 showing the prepaid cards are being utilised and provide real value for the underserved.

With a hint at the extended analytical capabilities available in open banking applications, the online portal allpay opened up for the Scottish government allowed for real-time reports on successful and unsuccessful transactions to see where the funds were being spent – providing improved auditing capability.

So, it's not such a leap to see how open applications can outline not just payments but capacity to pay – with all the implications in that for a post-pandemic public sector. And, in moving away from the 'old school', Killeen is keen on the potential open banking also offers for teaching the essentials of personal financial management. Social value at the tap of an app.

"Sure, the sector's response to Covid-19 is rightly recognised as bold. But the future's coming so fast it will soon be the past. We need to be bold enough to evolve and ensure no-one is left behind," said Killeen. TFT

AT A GLANCE

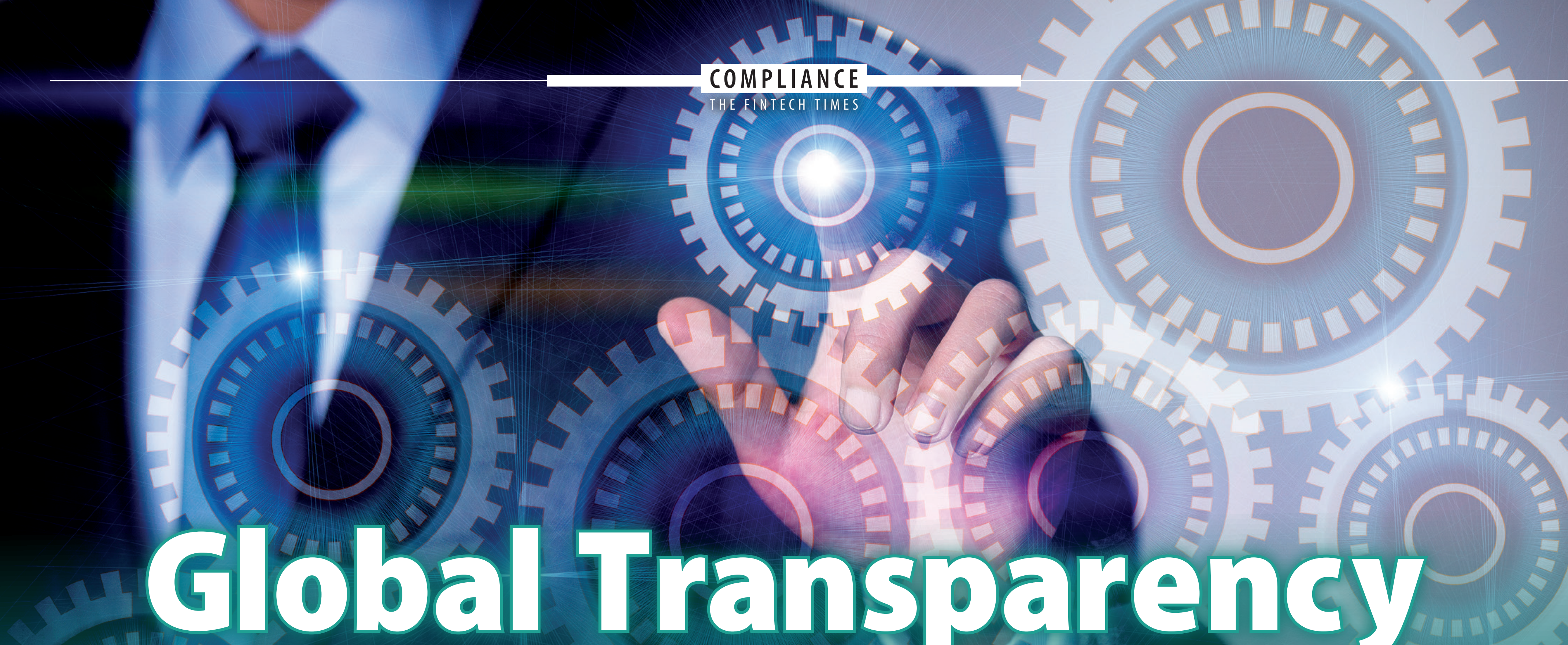
WHO WE ARE: allpay Limited is the UK's leading payments specialist. With its core business concentrating on providing bill payment services – primarily to the public sector – it handles around £8billion a year, across 80 million transactions.

Our aim is to work with each client to save them money through creating modern payment systems both cost effective and convenient for the end consumer.

allpay is committed to managing its growth responsibly to continue to make a positive contribution to the community and environment, as well the workplace.

COMPANY: allpay
FOUNDED: 1994
CATEGORY: Payment services
KEY PERSONNEL: Tony Killeen, founder, owner and managing director (above)
HEAD OFFICE: Hereford, Herefordshire
WEBSITE: www.allpay.net
LINKEDIN: linkedin.com/company/allpay-limited
TWITTER: @allpayGroup

allpay



Global Transparency

*January 2021 sees the launch of **Clarency**’s global business platform, **biz.Clarency**. The Singapore-based fintech has taken something of a sideways look at inter-country trade, focusing on an overall lubrication of the machinery rather than developing a one-problem solution.*

With **Bob Blower**, CEO, Clarency

Bob Blower, Clarency’s CEO, sees silo thinking as one of the greatest obstacles to easier and fairer global trade.

“Everyone has acknowledged that it’s not easy to deal between regions, especially when some of those regions are insular, or prone to corruption and risk, like many emerging economies. But none of these obstacles is the result of a single problem. We have to think more holistically if we’re going to open up the world.

“A couple of years back, we all started talking about KYC (know your customer), AML (anti-money laundering, KYCC (know your customer's customer), AFT (anti-terrorism funding) and KYCCC (know your customer’s customers and their customers) and a load of other acronyms that got created to describe some fintech’s ‘unique’ solution. Some of them were truly innovative but, almost without exception, none of them focused on the whole picture. That’s what we’ve set out to do with biz.Clarency.”

Rather than re-invent work that has already been completed and proven by other companies, Clarency has selected and partnered with solutions that have already proved their worth in specific fields.

“We looked for great technology, of course,” says Blower. “But even more than that, we looked for companies with the right attitude; people who were enthusiastic about being part of a complete solution, and who were willing to work with us to create it.”

Sitting behind biz.Clarency’s simple, logical user interface is leading-edge technology from the likes of ShuftiPro, ComplyAdvantage, InterlockLedger and China Systems.

Bob Blower has an interesting analogy. “Think of biz.Clarency as the conductor of an orchestra made up of very fine musicians. Carlos Kleiber couldn’t play the piano like Sviatoslav Richter. But with Kleiber conducting, they delivered the definitive rendering of Dvořák’s Piano Concerto.

“What we wanted to produce was the finished piece of music, not the brilliant but separate components that went into it. You wouldn’t enjoy Mozart, the Beatles or Taylor Swift if you had to log into a dozen separate streaming services for each instrument.”

> Creating a two-blockchain system that allows both parts to maintain their confidentiality while creating commercial transparency is exactly the sort of challenge biz.Clarency was created for

Blockchain has been a major buzzword throughout 2020, with seemingly every bank and fintech announcing some application of its secure and immutable technology. But is it the panacea that we’ve been told it to be?

“Blockchain is superb in its place, but it’s no magic bullet. “says Blower. “We use it in biz.Clarency for what it does best: to provide an unquestionable, immutable audit trail for every onboarding document, event and decision, along with the same level of diligence for every ensuing transaction. That means that any properly authorised regulator or law enforcement agency can examine any event chain with absolute surety that it’s viewing a true record. But blockchain was never intended to support dynamic, process-based activities. Try to make it handle situations like that and you end up with a clunky, awkward workflow, which was exactly what we set out to avoid.”

To achieve that level of immutability, Clarency has partnered with InterlockLedger, whose patented method of record locking has created a next-generation ledger that isn’t subject to the security defects that were discovered earlier this year in conventional blockchains.

“It’s been great working with the InterlockLedger team, not least because they understand where their technology fits. It provides the rock-solid base for our platform without getting in the way of the rapid, adaptable automation that we needed to develop to make international trade faster and easier, as well as more secure. To return to our orchestra analogy, the IL2 next-gen blockchain was never intended to be the first violin, but it provides the bass line without which everything else is just show.”

In a recent development, Clarency has begun working with Professor Wei-Tek Tsai on integrating, via the innovative blockchain solution he’s created, to provide compatibility with the new government-approved Chinese financial blockchain.

“This is a good example of what biz. Clarency sets out to do. It’s there to remove barriers to trade by providing end-to-end transparency of every stage and every actor in a business relationship. China is eager to trade, both in import and export, with the rest of the world. It understands the need for openness in those relationships, but at the same time wishes to be in control of its data. In fairness, that attitude’s actually not so different from the western world’s. Creating a two-blockchain system that allows both parts to maintain their confidentiality while creating commercial transparency is exactly the sort of challenge biz.Clarency was created for.”

The platform, which is already live in beta with test clients such as Eqibank and Reserve Trust, will be generally available from January 2021 to banks and other international financial institutions. TFT

About Clarency

Clarency is a major payments enterprise based in Singapore. It was acquired in 2020 by the Choice International Group, which has operated strongly in global trade finance, foreign exchange and international remittances since 2004. The acquisition of Clarency and the launch of the biz.Clarency platform sees the group moving forward as a fully-fledged fintech.

Website: www.clarency.com

Website: biz.clarency.com

LinkedIn: linkedin.com/company/clarency-com

Clarency

Farewell paper cheques, Hello digital payment fraud?

Digital uptake wallets and other payment methods have increased tenfold in the last year – but with new technologies comes an increase in potential fraud opportunities

Yinglain Xie, CEO of Datavisor

Digital wallets, peer-to-peer cash apps, automated clearing house (ACH) and debit cards. In just decades, these digital payment options have risen in popularity because of their convenience and the speed at which they enable money transfers. In 2020, Covid-19 and the urgent need to reduce the spread of infection has accelerated the adoption of digital payment methods. A casualty of this trend? Paper cheques.

The number of paper cheques has dropped roughly 1.8 billion a year, and at this pace, they're likely to disappear completely. Not only do paperless transactions reduce waste and processing time, they eliminate the risk of cheque fraud, which has risen 65 per cent since 2015.

According to the Federal Trade Commission, individual losses from cheque fraud are six times higher than losses from all other types of fraud, and in 2019, Americans reported more than 27,000 fake cheque scams with associated losses exceeding $28million.

But as paper cheques are replaced by digital payment methods, new challenges emerge. Digital fraud associated with cash apps, card-not-present (CNP) transactions and wireless transfers is also on the rise – and increasingly hard to fight.

With change comes challenges

People used to write paper cheques for many reasons – for example, to pay their gardener, piano teacher or other service providers. But social distancing orders deter face-to-face interactions, and today it's much more common for service providers to request money digitally.

Similarly, digital payments are a new standard for B2B organisations, as they look for ways to automate processes and reduce administrative overhead. Electronic invoice payments cost 60 per cent less than paper-based payments – and they're much faster, improving the recipient's experience with the organisation.

The total transaction value of digital payments is expected to reach nearly $4.8trillion and, in fewer than five years, half the world's population will be armed with a digital wallet. This rapid shift in the payment industry has put financial institutions at risk, because they lack experience and understanding about the methods fraudsters use to launch attacks through these new platforms.

Legacy fraud solutions must have access to historical data, in order to train their detection models to recognise suspicious activity. These solutions rely on rules and trained labels. Since many of the payment options people use are so new, historical data or trained labels just don't yet exist. Fraudsters constantly change their attack methods, and reactive solutions, such as pure rules-based systems, can't keep up.

What does digital payment fraud look like? It comes in myriad forms. A fraudster may use online marketplaces to collect money for non-existent goods via cash apps like PayPal or Zelle or use stolen credentials to create fake peer-to-peer (P2P) accounts for making purchases. If a fraudster has someone's account credentials, they can easily send a money request and most people will trust that it's legitimate. Fraudsters may take over bank accounts and issue ACH payments to their created accounts – which is hard to do with physical cheques but easy now that everything's digital.

Compounding the problem, new payment options are being introduced to market in rapid succession. For example, in the digital wallet market, PayPal and Venmo were two of the earliest players, followed by Google Pay in 2011, Apple Pay in 2014, Samsung Pay in 2015 and Zelle in 2017. Now a plethora of apps are available: GrabPay, Touch 'n Go, vcash and more. Reactive methods of fraud detection can't keep pace with the rapid innovation occurring in this space – and this leaves users and their financial institutions extremely susceptible to fraud.

Digital payments are vulnerable, but they also enable better insights

With paper cheques, transactions are local, and often involve face-to-face contact that makes fraud difficult or impossible, for example, when you hand a check to your gardener. Digital transactions lack those safeguards. However, it's not all negative. Whereas the digital payment format might make it easier for bad actors to commit fraud, it can also make it easier to catch them in the act.

In paper-based processes, data collection happens in siloes. For example, people accepting account applications don't exchange information with those collecting cheques, and data can't be correlated to reveal patterns. On digital channels, it's much easier to close that gap.

About Yinglain Xie

Having previously worked at Microsoft, Yinglain Xie has more than 10 years of experience in security, specialising in fighting large-scale attacks with artificial intelligence and big data technologies.

The proactive approach should be taken, which differs significantly from how legacy rules-based fraud detection works. Rather than learning everything about a past threat or certain fraud type and creating rules and labels based on what's happened in the past, it is time for us to adopt a proactive approach that analyses all data holistically and applies predictive analytics to treat the root cause of the problem at the account level before a specific attack is successful.

In addition, advanced algorithms that learn and adapt in an unsupervised manner can be used to flag suspicious activity, even if the patterns are unknown. So-called unsupervised machine learning (UML) algorithms will be especially critical as innovation in the payment industry continues to accelerate. Altogether, by centralising intelligence from every customer interaction – account applications, payment transactions, device intelligence, user behaviour and more – you can leverage advanced machine learning techniques to identify unknown, fast-evolving patterns of fraudulent activity in real-time.

Get a step ahead of payment fraud

As cheques disappear and new digital apps emerge, fraudsters will continue to find ways to exploit them. But with a proactive approach, organisations can protect themselves from unforeseen attacks. Rather than waiting to find out what fraudsters have up their sleeves, use the unique characteristics of the digital payment format to gain actionable insights and cut fraudsters off at the pass. TFT

There are some things money can buy - for everything else there's cybercrime

We mostly associate cybercrime with the loss of money, estimated to be a $1trillion per year drag on the global economy and growing. But my biggest worry is not money. Cybercrime's biggest threat is to our values and principles, the things money cannot buy.

Chris Ganje, Founder and CEO of AMPLYFI

Whether hacking accounts, stealing private data, or holding systems to ransom, financial loss is the standard measure of cybercrime. Awful though this is, cybercrime in this form does not undermine our society directly. Indeed, providing individuals take basic digital security precautions, then the likes of Mastercard and Visa will generally handle the losses. But what about democracy, a free press, or equality?

At AMPLYFI, we study the deep web. Away from the reach of consumer search engines it holds 95 per cent of the internet's data. However, the breeding ground for much cybercrime is the dark web. Here, unlisted, encrypted sites allow people to trade untraceable cryptocurrencies for illicit goods or services. These activities are hard to track, quantify and control.

Our analysis of the deep web suggests that the next decade will be the most prolific ever for cybercriminals. The basis for our hypothesis is that cybercrime has emerged in lock step with digital transformation. Put simply – the more value that goes online, the more attacks are leveraged there.

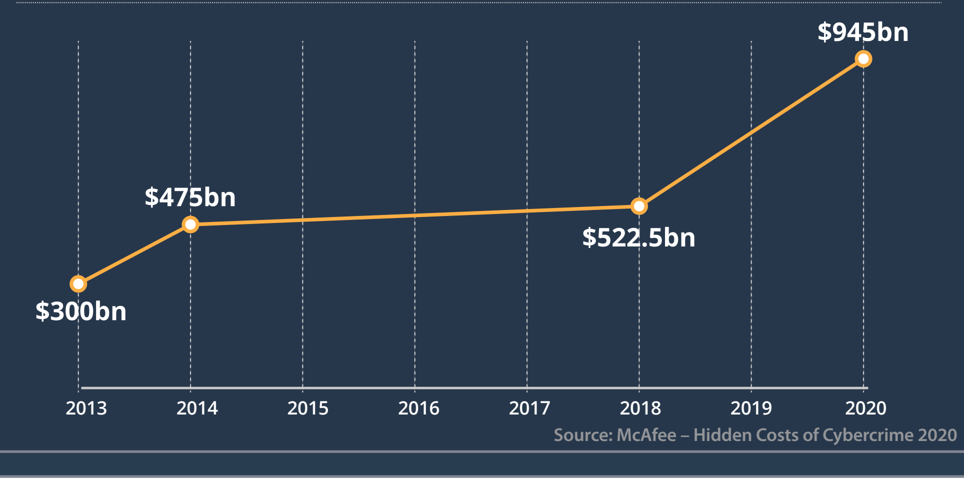
But the impacts are not confined to balance sheets and bank accounts. In a survey by McAfee (global security firm), 92 per cent of respondents reported feeling effects from cybercrime that went beyond pure monetary losses. The lack of understanding of these ‘non-financial losses' is worrying in itself, but 56 per cent of respondents also shared that they have no plan to prevent and respond to a cybersecurity incident. Until this metric moves, the impacts of cybercrime will inevitably increase.

Of growing concern is the loss of trust that results through stolen IP, fake news and destabilised democracies. A new Cold War is breeding a cabal of ‘digital arms dealers' whose ‘back-doors', troll farms and ransomware are powering the geopolitical aspirations of shadowy non-governmental organisations.

Since medieval times, codes, cyphers and hidden messages have been used to influence global change. When communication went electronic, the solution became technical. During World War 2, at Bletchley Park in the UK, Alan Turing developed early mechanical machine-based technologies to break Germany's ‘the unbreakable' Enigma code. Tommy Flowers, an engineer at the British General Post Office (GPO), then built Colossus, the first electronic programmable computer to decode the even more complex Lorenz code. The UK's Government Communications Headquarters (GCHQ) the successor to Bletchley Park, went on to develop an early version of the now-ubiquitous ‘RSA asymmetric public key encryption' in the 1970s. In the mid-1990s military researchers in the US created ‘The Onion Router' (or Tor), which paved the way for the aforementioned dark web.

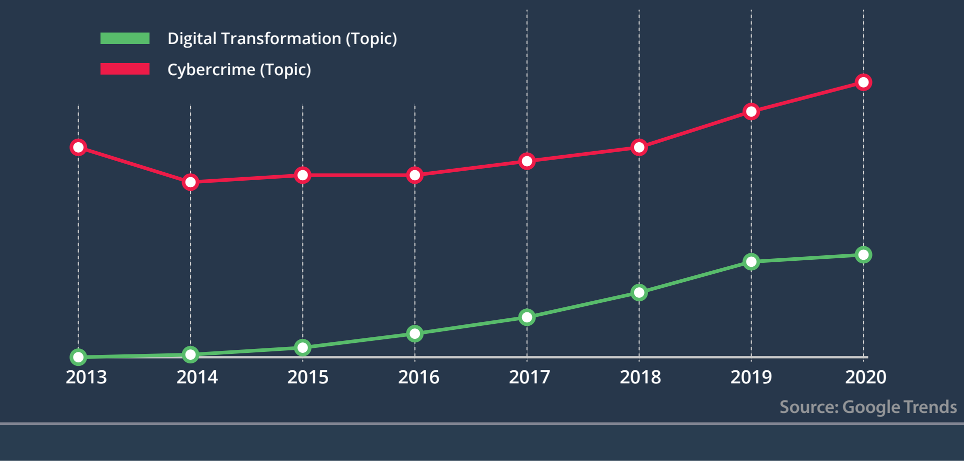
Gradually, a wave of state sponsored cyber innovation spiralled out across the

Estimated Costs of Cybercrime 2013 to 2020



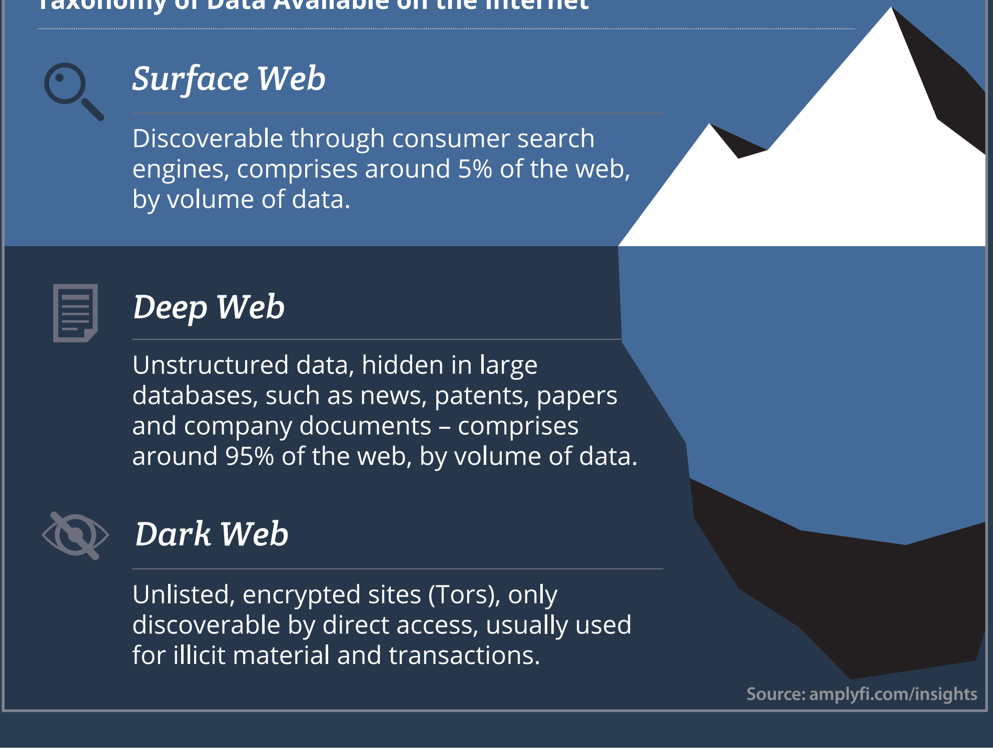
Source: McAfee – Hidden Costs of Cybercrime 2020

Digital Transformation & Cybercrime Topics Global Searches 2013 to 2020



Source: Google Trends

Taxonomy of Data Available on the Internet



Surface Web

Discoverable through consumer search engines, comprises around 5% of the web, by volume of data.

Deep Web

Unstructured data, hidden in large databases, such as news, patents, papers and company documents – comprises around 95% of the web, by volume of data.

Dark Web

Unlisted, encrypted sites (Tors), only discoverable by direct access, usually used for illicit material and transactions.

Source: amplyfi.com/insights

globe to Russia and China and more recently, in guerrilla form by groups, such as the Islamic State. Much like the Cold War, that has extended into a conflict of values. Beyond finance and the state, to society itself, pitting Conservatives against Socialists, Brexiteers against Remainers, and now Vaxxers against Anti-vaxxers. Suddenly, nuclear submarines are not the hottest threat, when a troll farm can do so much more damage, with so little cost.

Whether stealing assets, disrupting processes or manipulating people, cybercrime is continually evolving. Digital innovations are being mutated into multi-nodal threats spanning everything from WhatsApp to Intel microprocessors. As digital transforms more of our lives, these nodes are likely to multiply even further.

Added to this, the growing pressure for organisations to embrace the digital economy is irresistible. The early innovators, now far ahead in their market capitalisations, took risks that bought them time to develop and stress test systems. They have knowledge of the technical and social engineering dynamics of emerging attacks, including the constant weak link, humans. The Enigma code was ultimately breakable because of the human elements – people transmitted repetitive words that allowed codebreakers to build patterns faster.

Finance organisations have long known that security includes shaping customer behaviour, other sectors are learning this the hard way. User convenience is often the weak point, but how do we engineer secure systems that users can still access? Writing passwords down has long been an issue and current password managers and weak two-factor authentication systems are likely to cause many of our future issues or slow us down. If the single alpha-numeric password is now almost redundant, do we move to security keys based on images, feelings, or analogue data, such as physical properties? How else will we make the billions of internet of things (IoT) devices secure, or trust our driverless systems as they hurtle down our roads? Getting the balance right between convenience and security is clearly an area where the financial service sector can lead.

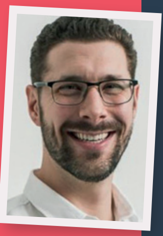
The onset of other technologies, such as quantum computing, will also cause disruptive ripples, as encryptions designed over the decades will be eclipsed by new emerging technologies just as Tommy Flowers' computer showed. Ultimately, this is a race between legacy technologies and new ones. But what can be done about it? Or, perhaps more pertinently, what will commercial organisations be allowed to do? Even when virtually unbreakable systems are possible, governments discourage them, fearing that it will enable criminals to exploit the anonymity provided. This is a bigger question for society – do we value more privacy or more security?

There are also societal questions when fast growing foreign organisations become critical to national infrastructure, such as Huawei in the EU and US. At scale, an extended disruption, with the cascading effect on national infrastructure could feasibly cause substantial disruption on the scale of other 'Black Swan' events. If so, perhaps, a bit like the theft of money, we need to have systems able to accommodate the equivalent of someone breaking into the odd safe, providing the entire house of cards doesn't collapse along with it.

Ultimately, at AMPLYFI, we believe it wise to assume that cybercrime is inevitable. Though assigning the resources to mitigate them can be a tough pill to swallow. As with many things digital, the experts are often not old enough to be in your boardroom, let alone take a role as chief information security officer (CISO). Indicating that sourcing experienced talent in this space is likely to become highly competitive.

Dealing with these potential disruptions will require a broad organisational view. Just as siloed 'IT' morphed into digital teams and 'informatics' into data science, information security will need to transform to deal with this change. It will need a systematic approach to not just individual cyber threats but how they combine to combat multi-nodal threats. Every branch of an organisation will need to become aware of all forms of cybercrime and cybersecurity. Because if you can't buy it, then someone will definitely be trying to steal it. TFT

About Amplyfi



Founder and CEO of AMPLYFI, Chris Ganje is a pioneer in the application of machine learning and data science across structured and unstructured data sets, helping organisations make decisions based on real world information, without the bias of human analysis. Chris is a BP plc alumni, where he was responsible for leading the Group's disruptive technology work and developing its European energy technology policy initiatives. He is a fellow at Cambridge University's Centre for Science and Policy, and joins the Innovate UK national advisory board in 2021.

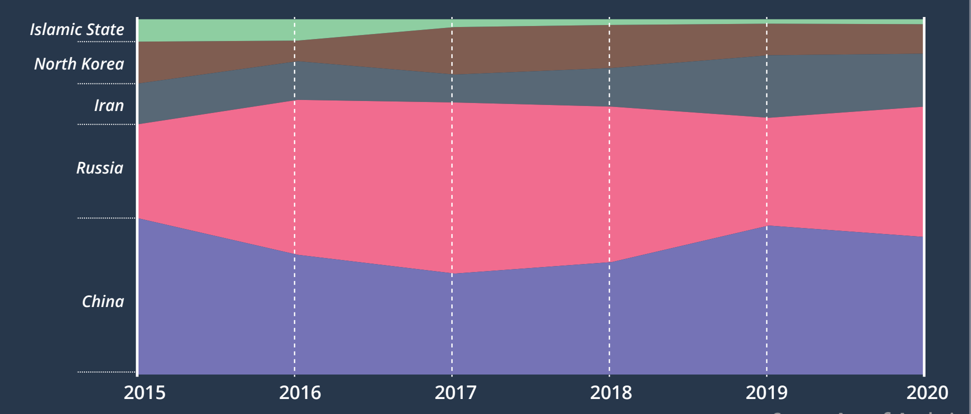
Website: www.amplyfi.com

LinkedIn: linkedin.com/company/amplyfi

Twitter: @AMPLYFItech

AMPLYFI

Proportional Strength of States Association with Cybercrime 2015 to 2020



Source: Ampyfi Analysis

Common Cyber Threats

Source: Cisco

Malware
Malicious software, including spyware, ransomware, viruses and worms used to exploit compromised systems.

Phishing
Sending fraudulent communications that appear to come from a reputable source, to gather sensitive data from recipients.

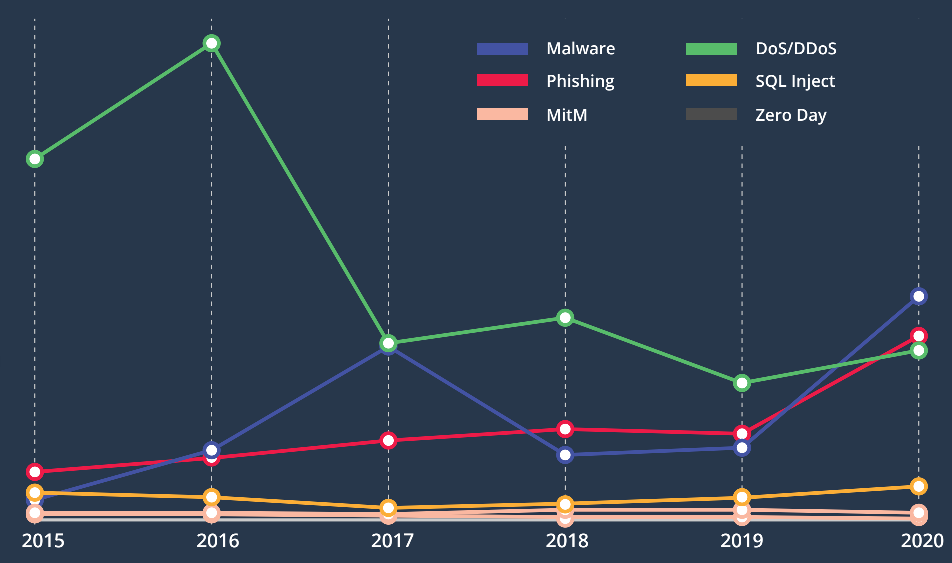
MitM
Man-in-the-middle (MitM) or eavesdropping attacks, attackers insert themselves into a two-party transaction and exploit the data shared.

DoS or DDoS
Denial-of-service (DoS) attacks floods systems with traffic, sometimes using other, compromised devices (a Distributed-DoS).

SQL Injection
Structured Query Language (SQL) injection is when an attacker inserts malicious code into a database e.g. via a search box.

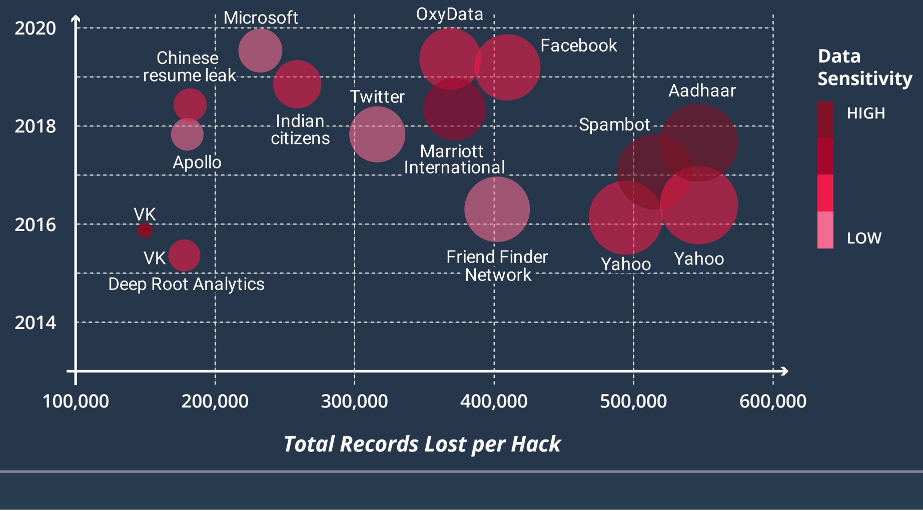
Zero Day Exploit
Attacks that happen after a software vulnerability is discovered but before a patch or solution is implemented.

Comparing Significance of Cybercrime Attack Types 2015 to 2020



Source: Ampvlyfi Analysis

Top 10 Data Breaches by Records Lost due to Poor Security 2016 to 2020



Source: Data is Beautiful

LET US ENTERTAIN YOU

Despite global disruption, the shows go on for international events and media empire SiGMA

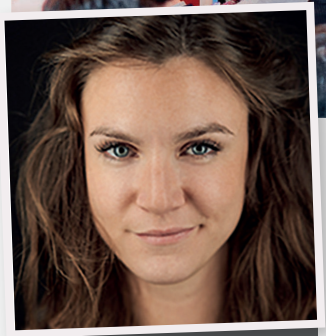
SiGMA is an international events and media company encompassing the world of gaming both online as well as land. Its international events are world-renowned for bringing together entire industries to educate, debate and network in a unique and dynamic environment. Currently operating in four continents (Europe, Asia, America and Africa), SiGMA brings together leading suppliers, operators and affiliates in events that are at the forefront of shaping the future of the global gaming industry in an informal yet business focused B2B environment.

SiGMA World Gaming Festival embraces all three verticals – affiliates, operators and suppliers – because today's super affiliate is fast becoming an operator, thanks to lower barriers to entry.

SiGMA is held in different emerging gaming hubs throughout the globe and the aim is to merge two large expos – SiGMA and AIBC – under one roof, pushing boundaries for the two verticals to learn and feed off each other. In these events one can expect keynote speakers and innovations in blockchain, artificial intelligence, big data, quantum computing, internet of things (IoT) and fintech to enlighten the crowd about the future.

SiGMA Europe

SiGMA Europe is an annual iGaming conference in Malta that gathers top speakers and the most interesting exhibitors of the gaming world. Europe remains a leading market for gaming, making SiGMA Europe the perfect opening gaming show for 2021 in addition to inaugural shows across Asia in May 2021 and the Americas in September 2021.



Sophie Crouzet, Chief Operating Officer at SiGMA

SiGMA Asia

In line with SiGMA's commitment to cover the various gaming verticals, the company has capitalised on the strong interest in Asia for gaming and the growing value for companies looking to move into up-and-coming gaming markets. The Philippines is positioned at the heart of Asia's gaming sector, with the regulator PAGCOR defining the sector with solid regulation and clear industry leadership, making Manila an ideal choice for SiGMA's inaugural Asian supershow. The SMX convention centre in Manila is expected to have land-based, online gaming & emerging tech exhibitors, a cutting-edge conference with a line-up of speakers made up of final decision-makers and a plethora of networking events to facilitate business among the delegates.

SiGMA Americas

From the exploration of new markets to fresh digitisation, the emerging LatAm gaming market is also truly an exciting place to be. SiGMA Americas offers an open-door approach to innovation within Latin America's fast-changing gaming landscape as well as the established North American landscape.

The company is heading to the metropolis of Sao Paolo in Brazil for the next edition of its world-renowned show. SiGMA LatAm like all other expos also aims to combine both the gaming and emerging tech industries under one roof. The event will take place on 13 to 14 September 2021 at the beautiful Tivoli Hotel.

SiGMA Africa

Although retail gambling still dominates Africa, online gambling has been on the rise. Africa stands out as a region attracting significant interest from stakeholders across the global gambling industry. Tech-savvy and diverse, there are plenty of new opportunities to be found in the gaming and emerging tech sectors, which is why SiGMA is heading there in 2022. Africa was the only reasonable next step for our growing portfolio of events as we solidify our presence in the global gaming industry.

During these unprecedented times, SiGMA also introduced the future of live conferences with its digital events. After extensive research, and the success of three virtual events throughout 2020 (SiGMA Asia, SiGMA Americas and SiGMA Europe), the virtual expos, having combined the SiGMA and AIBC brands to bring a one-stop destination, proved to be a huge success. The virtual expos delved into updates in regulation and how they can affect individuals, the new reality of affiliation and marketing, the changing faces of sportsbook and payments, the freshest emerging tech and more.

Following a very successful run, SiGMA is also looking to present the fifth edition of SiGMA Pitch this year during its events. More than 100 startups will be selected to showcase their products and initiatives throughout the event. Each startup will have a small booth at SiGMA surrounded by top investors and mentors. However, only the judges' top ten makes it to the Pitch during the final leg of the Summit.

SiGMA has recently revamped its website, currently available in six languages so far with another four coming soon. The company's website is a one-stop shop that keeps on top of the latest developments from across the world and its dedicated in-house team of media wizards create premier online content to keep you informed in style.

The efforts of a strong content and media team at SiGMA, brings up-to-the-minute updates and a selection of periodically published magazines, catering a news platform that highlights the developments of the industry. The SiGMA content team is made up of highly proficient native speakers, who understand the dynamics of the language and its value to the client. The quality of writing and the clarity of message remains of the highest priority to the company.

Positioned at the cutting edge of a very competitive industry, the event has evolved since 2014 into the definitive gaming showcase, operating on a world stage. TFT

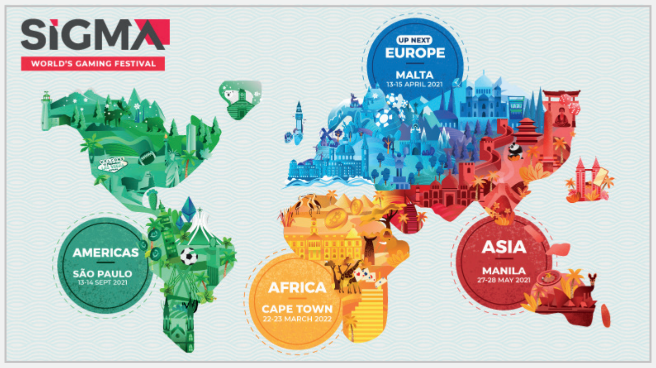
Join SiGMA Group for the seventh edition of SiGMA at the MFCC – Malta Fairs & Conventions Centre and explore how you can benefit from being a delegate, sponsor, exhibitor or a keynote speaker. For more info about SiGMA's events, get in touch with Sophie at **sophie@sigma.world**

Website: www.sigma.com.mt/en/home

LinkedIn: linkedin.com/company/worldsgamingfestival

Twitter: @iGamingSummit

SiGMA



Transforming payments for vulnerable people

It's important to balance the benefits of digital channels with ensuring financial inclusion

Justin Pike, Founder & Chairman of MYPINPAD

Covid-19 has rapidly accelerated digitisation of the customer experience, particularly with respect to how consumers shop, pay and bank. The shift to digital channels has been an important lifeline for many consumers, providing access to essential products and services during a time when physical contact must be significantly reduced or eliminated.

But the pace of digital evolution this year has brought two significant issues to the fore – an increased risk of fraud, and an urgent need to address the barriers some consumers face in accessing digital and financial services, that have resulted in them being financially excluded. A lack of financial education, physical restrictions, limited access to technology, and security concerns are some of the factors that have prompted the industry to invest more effort and ensure that financial services products are accessible, secure and meet the needs of all consumers, irrespective of age, financial status, disabilities or any other factors.

As Covid-19 continues to change daily life, possibly for some time to come, how do we balance the benefits of digital channels while ensuring financial inclusion and protecting everyone against fraud?

DIGITAL ADOPTION AND THE RISK OF FRAUD

The shift to digital has been happening for years; even before Covid-19 cash transactions represented only 23 per cent of all payments in 2019, according to UK Finance. And digital transformation has fast become a strategic imperative for any business seeking to remain relevant, enabling a technology-driven digital experience across multiple touchpoints, channels and devices, whenever and wherever consumers need it.

Furthermore, regulatory changes have also played a key role in encouraging digital innovation and security, while also incentivising further developments for the benefit of the consumer. For example, changes to strengthen security and authentication standards are a crucial step in ensuring all customers can securely access financial services with great confidence.

As a result and unsurprisingly, the risks of fraud have dramatically increased in light of more digital offerings and cashless transactions, and despite changes in regulation such as extending the contactless limit. In fact, UK Finance released a warning that criminals have been exploiting and adapting to the opportunities Covid-19 has enabled.

An example of this is the closure of TSB branches across the country. Impersonation scams – where fraudsters pose as bank staff – almost doubled in the first half of the year, rising to 15,000 at a £58million cost to victims, and it hasn't dropped yet. Conducting its own research on the topic, TSB found that more than a third (37 per cent) of Brits would respond to at least one fraudulent message claiming to be from their bank, which indicates just how convincing these scams can be.

Against this backdrop, we acknowledge the importance of working collaboratively as an industry to collectively and continuously ensure consumers are educated and aware of the latest online fraud and security threats, and how to prevent them.

WIDER DIGITISATION IMPACTS THE ELDERLY AND VISUALLY IMPAIRED

While digital evolution brings a degree of risk for all consumers, there are groups of people who are more at risk in a digital environment than others. As pioneers for technological innovation that impacts consumers, we must be mindful of the risks posed to those who are most vulnerable.

The highest risk group is elderly people, who are not only high risk when it comes to coronavirus but also tend to be most negatively impacted by the shift to digital. This is for a multitude of reasons, not the least that many simply aren't as tech-savvy as younger digital native generations. They also tend to be less trusting of financial technology due to a lack of familiarity with digital processes, information overload or underlying health issues, which makes them less eager to adopt.

If we look at the UK as a case study, prior to the pandemic roughly four million over-65s did not use the internet at all, according to Age UK. And, while Mintel has found that 43 per cent of those in this age group have now shopped online, there are likely some who still struggle to adjust to making payments and managing finances digitally.

Physical restrictions, such as visual impairments, can also impact adoption, which is a prominent route to financial exclusion – using small screens can be challenging and dexterity issues can hinder the ability to use mobile phones and pin pads. Blindness and visual impairment affect at least 2.2 billion people around the world, so it is essential that the digital solutions being developed are inclusive for people of all abilities.

In 2018, a blind woman made headlines when she lodged a lawsuit against Commonwealth Bank of Australia over its 'inaccessible' touchscreen-only Albert POS terminal, which she said was so difficult to use she often needed to share her PIN with shop staff. This is a particular area of focus for MYPINPAD.

THE PAYMENTS INDUSTRY'S ROLE IN SUPPORTING VULNERABLE PEOPLE

As an industry, we have a responsibility to tackle the challenges facing all consumers,, and especially those more vulnerable groups, And, while the threat of online fraud is present for everyone, as we continue to develop more financial offerings and services that better serve the individual, we must ensure that everyone can access and benefit from these.

MYPINPAD's founding purpose was to enable the most trusted, secure authentication platform, free of legacy constraints, for everyone. We imagined a world where customer experiences, such as payments and identification, which must be secure and are inherently full of friction points, could be innovated and transformed to create a better experience for consumers. And this means equal access for all people, regardless of age, stage, race and ability.

Now, more than ever, our purpose is right at the heart of everything we do, especially as smart devices with stronger security standards continue to play an increasingly vital role in supporting our society. As we develop solutions that not only unlock opportunities to innovate and improve customer experiences, such as payments, but are also secure, cost-effective and scalable, ensuring they are inclusive for everyone is at the forefront of our thinking.

Payments regulators have identified stronger authentication standards for 'PIN on Mobile' as developed by MYPINPAD, which enables smart devices to become financially inclusive payment and authentication tools. From contactless payments and new regulations to improved authentication measures and seamless user experiences, global financial inclusion payment innovations hold the key to improving the way we transact online now and in the future. TFT

About MYPINPAD

MYPINPAD's vision is to enable the most trusted, secure, fraud free authentication platform, free of legacy constraints for everyone. We imagined a world where customer experiences, such as payments and identification, could be innovated and transformed. Where any experience that required the authentication of a person could be securely done on an everyday mobile device, which would therefore open up a world of possibilities to innovate the customer experience.

Website: www.mypinpad.com

Linkedin: linkedin.com/company/mypinpad-ltd

Twitter: @myPINpad

MY PINPAD

Rayissa Armata, Head of Regulatory Affairs at IDnow

KYC compliance beyond Brexit

Addressing the immediate consequences of Brexit for UK businesses operating in Europe

The exit of the United Kingdom from the European Union (EU) delivered many new decisions, functions and costs for UK-based corporations operating or considering operations across the EU.

Since 1 January 2021, the UK is considered a 'third country' in its relations with the EU and, as such, it has had significant implications for financial institutions and other reporting entities' business models, structures, and compliance requirements. Namely, companies must continue to meet national and EU anti-money laundering (AML) and know your customer (KYC) regulations. The ability to 'passport' UK legislation and practices across the EU's internal borders is no longer available to UK firms and, in order to meet equivalent standards and regulations, businesses must be ready. This means companies need suitable partners and must make adjustments where they are needed.

While an EU member state, UK-based companies simply had to demonstrate compliance by following and adhering to EU AML and KYC regulations and law, even passporting into the EU. However, once the Brexit transition completed on 31 December 2020, the UK lost its status as a member of the EU. With this loss of status, the UK no longer has access to simplified verification and enhanced due diligence checks are required to fulfil newer AML amendments and requirements.

For UK companies that onboard customers in the EU, they are required to follow local laws and regulations specific to individual countries. In so doing, they also have to ensure that, no matter which country their customer is based, their AML and KYC regulatory standards must meet or exceed those of the UK.

Additionally, for many UK companies, the degree of change post-Brexit depends on their current European footprint. To further this thought process, the type of business or industry sector they represent, and their own resources to operate entities or subsidiaries across the EU must be considered. For businesses that are obliged under AML law, notably in the banking and financial sectors, insurances, mobility, telecoms and online entertainment/gaming, several factors must be taken into account in order to fully understand the scale and extent that Brexit affects their business.

Over the past few years, firms have been considering several factors that would affect their operations post-Brexit. These include:

- Loss of passporting – establishment of automatic cross border
- Their prudential framework
- Revisions to capital structures, provisions and services
- Revisions to their legal entity structures
- How to implement and learn the different AML/KYC regulations
- Data protection
- Potential implications for holding or transferring data
- Legal arrangements
- Tax considerations
- Restructuring client relationships

Four of these issues are most pressing, so let us discuss in more detail; passporting, relocation, KYC obligations and data privacy.

OPERATIONAL CHANGES: PASSPORTING IS NO LONGER AN OPTION

Passporting allows a financial entity to establish a branch in one EU member state in order to provide direct cross-border services across the European Economic Area (EEA). Supervision is primarily carried out by the home country unless specified.

However, the current use of passporting no longer applies to the UK after 31 December. As such, authorisation requirements will need to be met under European and Member State law. This will be a challenging, yet feasible, path for UK businesses.

> IDnow's experience is shared in setting global standards through extensive collaborations with national regulators and organisations, such as the European Telecommunications and Standards Institute (ETSI), the Financial Action Task Force (FATF) and the FIDO Alliance

UK firms may need to get authorisation from competent authorities among EU member states to access the EU market (i.e. setting up subsidiaries). They have to comply with both UK and host country regulation to conduct regulated activities, and EU firms, in turn, need to become authorised by UK authorities to access the UK market.

RELOCATION, RELOCATION, RELOCATION

As third country status begins, the UK government will have to make significant efforts to develop new trade agreements with individual member countries. Cross-border entities may have to restructure and UK entities are going to be impacted especially considering the UK's strength in investment banking, where passporting has been critical across the EU.

These changes may require significant changes to an entity's investments in capital, staff and infrastructure and as a consequence, banks may need to transfer parts of their UK based business to existing or new EU locations.

KYC OBLIGATIONS: MEETING COMPLIANCE REQUIREMENTS ACROSS EU AMLD5

For businesses in the banking / finance industry, as well any entities obliged to follow AML laws, KYC screening is compulsory. Heavy fines and penalties leave little room for non-compliance, and obliged industries must have measures and procedures in place to meet these requirements.

Within Europe, national AML laws can vary and UK businesses must ensure they can meet KYC procedures that are permissible in a particular member state. Member states follow a combination of guidelines established under the Financial Action Task Force (FATF), implementation of AML Directives, the latest being AMLD5 and the upcoming AMLD6 and national AML Acts.

The AMLD5 and AMLD6 aim to bring greater uniformity in AML / KYC compliance within the EU. While the 5th Directive was implemented before the UK's Brexit deadline, the UK will have to follow its own laws under its own authorities. This forces all compliance operations to understand what these differences are and how it will affect their corporations' business obligations.

In 2020, the 5th Directive introduced changes across several EU member states, introducing stricter adherence for AML legislation, widening the types of institutions that must comply with AML law, amendments to the use of digital KYC solutions, and cross border services for trust services under the eIDAS Regulation.

Although the UK currently complies with legislation in force within the

EU and will need to implement the 5th AML Directive, member states and their regulators have variations in their interpretation of how the rules are applied in their jurisdictions. Corporations will need to review their existing structures and determine how they can continue to serve existing clients in the EEA regions.

For example, financial institutions routinely need to elevate their AML/KYC standards in order to satisfy various requirements. For some reporting entities, the differences in digital KYC compliance results in significant uplifts that requires new partners to meet such changes. (i.e. video identification in Germany vs automated KYC in UK).

Money laundering, terrorist financing, drug trafficking and identity fraud continue to be real threats. Efforts to combat these risks have become stricter and more focused. Inherent risks in using regulatory loopholes between Member States existed prior to Brexit and could pose even greater risks if entities such as banks, financial institutions, online entertainment such as gaming, e-commerce and other institutions are not prepared.

DATA PRIVACY AND GDPR

The exchange of customer data between corporations in the UK and EU mandates corresponding arrangements when it comes to data protection and privacy. The EU has stated that it is willing to grant unimpeded access to UK-based financial corporations only if they are subject to equivalent privacy and data laws as the EU.

UK businesses operating in the EU should consider how they address data transfer in order to clarify any outstanding issues. For example, financial and other reporting institutions should ask themselves a number of questions:

1. Can your existing customer data be transferred to a new jurisdiction or will a new KYC profile need to be created altogether?
2. How will this impact your existing client relations?
3. What are the costs involved to meet regulatory compliance?

Throughout this process, protecting the existing client experience should be of paramount importance and any refresh of client KYC data due to the UK exit from the EU will be critical. A due diligence process that is cost effective and ensures a client friendly process must be secure and client friendly.

THE CRITICAL ROLE OF THE IDENTITY VERIFICATION PROVIDER

Selecting the right identity verification partner for the pre-and post-Brexit journey is critical and can help firms navigate Brexit uncertainties. An identity verification-as-a-service (IVaaS) provider that operates across Europe and that has software built on some of the strictest regulations, (i.e. Germany's Federal Financial Supervisory Authority (BaFin)), can easily meet European regulations to onboard customers.

As a top tier software solution provider and leading European identification verification provider, IDnow offers identification solutions that meet the highest levels of security and fraud detection requirements within strictly regulated digital markets in finance and banking, insurance and telecoms. It has one of the world's most advanced infrastructure verification as a service IVaaS platforms that can verify in real time the identities of more than 4.3 billion people from 65 different countries. It also seeks to advise select Working Groups within the European Commission engaged in digital identity and verification standards across centralised and national levels.

IDnow's experience is shared in setting global standards through extensive collaborations with national regulators and organisations, such as the European Telecommunications and Standards Institute (ETSI), the Financial Action Task Force (FATF) and the FIDO Alliance. Its goal to keep the connected world a safer place is mission critical. IDnow serves to meet AML compliance and fight fraud. TFT

About IDnow

We are IDnow. The identity verification platform. Built for security. Loved by people. Our solutions are compliant throughout Europe and enable the highest level of data security. In the area of video identification of customers and electronic signatures, we were the first to provide the market with a legally secure solution without additional hardware. In May 2016 the IDnow video identification process was patented by the EU.

Our offer is directed at all business customers who would like to provide customer identification and contract conclusion online, such as banks, telecommunications companies, Fintechs, etc. Our customer portfolio includes renowned firms, such as Commerzbank, UBS, Sixt neuwagen, Telefónica and N26.

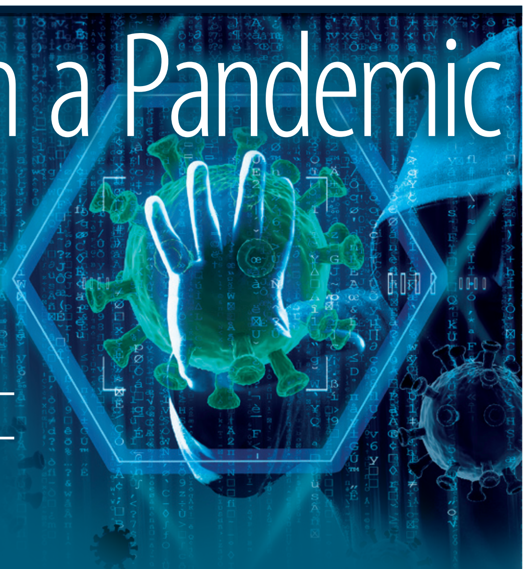
Website: www.idnow.io

Website: www.linkedin.com/company/idnow

Website: @IDnowGmbH

IDnow

Payments in a Pandemic



With rising fraudulent transactions, a focus on security is more important than ever

Danny Chazonoff, COO at Paysafe

It's no secret that the potential for fraud increases during a crisis and the turmoil created by Covid-19, with its combination of both financial and health threats, has created the perfect storm for fraudsters loitering in the wings.

Before the pandemic, the security of online payments was already paramount for both consumers and businesses, even when compared with user experience and convenience. We have been tracking the views of businesses and consumers on the security of financial data and their fears of being a victim of fraud for a number of years through our *Lost in Transaction* research series.

Back in 2018, 74 per cent of businesses told us they felt targeted by fraudsters – more than the previous year – making security a key criteria for more businesses (59 per cent) than any other when considering payments providers. In the same year, 59 per cent of consumers told us they felt uncomfortable sharing their financial information online to make a payment and in 2019, more than half (56 per cent) of consumers said they were concerned that switching from passwords to biometric authentication for digital payments would result in a dramatic increase in fraud.

Despite the world being shaken to its core by the arrival of Covid-19, online payment security remains the primary concern of businesses. In fact, it has become even more of a concern than ever.

PAYMENT FRAUD DURING COVID-19

In September 2021, we commissioned independent researchers to gauge the views of 1,110 online businesses based in the UK, US, Canada, Italy, Germany, Austria and Bulgaria on how they had been affected by Covid-19, as well as the trends they had seen emerge in shifting consumer behaviour within their online checkout.

More than half (55 per cent) told us that an increased risk of fraudulent transactions has been one of their greatest concerns during the pandemic. And, this is reflected among their customers; 60 per cent of businesses believe that consumers are more concerned than ever about being a victim of fraud and 68 per cent of businesses believe that consumers are increasingly looking to make payments online using methods where their financial details are not shared as a consequence.

This is already impacting the way consumers are paying online. Seventy-six per cent of online businesses said that they have already noticed a change in the way people pay, such as a greater percentage of consumers using digital wallets or ecash and, when asked why, the most popular answer from businesses was that consumers are looking for a more secure method of payment.

Our previous research, published in May, *Lost in Transaction: The impact of Covid-19 on consumer payment trends*, indicated that protection against loss from fraud (identified by 34 per cent of consumers) and financial data being kept safe from fraudsters (identified by 32 per cent) were the top two reasons people chose a particular payment method.

And, when we asked consumers, we also discovered that overall they didn't feel as though their online payments were secure enough. More than half (51 per cent) said they would accept whatever security measures were required if it kept their data secure – however poor it made the user experience – and another 25 per cent said they would accept a more inconvenient payment method than they currently use. Only 18 per cent said the balance between security and convenience struck by payment methods was currently correct.

NEW ONLINE CONSUMERS ARE SHIFTING THE LANDSCAPE

There are other reasons why payment security has topped the list of concerns this year. Covid-19 has definitely accelerated the adoption of commerce – our research showed 18 per cent of consumers are shopping online for the first time following the pandemic and concerns about sharing financial details with online merchants is one of the key reasons these customers have not shopped online previously. In addition, there is another group of consumers that only shopped online with a select group of businesses that they had a personal relationship with; now they are open to shopping online more they are inevitably interacting with merchants they are unfamiliar with and their willingness to share financial details has shifted accordingly.

For online businesses that want to attract and keep customers from these two groups, offering a choice of secure payment methods will be essential. At a time when customers are more valuable than ever, businesses don't want to be running the risk of losing out on revenue by losing customers that are changing their preferred payment method due to security concerns. TFT

Despite uncertain times and global disruption, cybercriminals have become increasingly adaptive to achieve success, says ***Jason Johnson****, Co-Founder at* ***Predatech***

Common security challenges facing fast-scaling fintechs

After a year of unprecedented business disruption that has forced many businesses, including fintechs, to undergo significant IT transformation, security is once again leading news bulletins.

The mass adoption of remote working has introduced a new series of security concerns, adding to the long list of security challenges faced by fast-scaling fintechs when it comes to securing their data.

Technological complexity

Fintechs are, as you would expect, a very attractive target for attackers, as they typically hold a lot of sensitive data. Account details alongside personal data are just two examples of the juicy information attackers are looking to sink their teeth into.

We're unlikely to see this change as financial technology becomes increasingly intricate and data rich. And, as the applications have become more complex, the required skills and resources required to secure them have also increased.

The growing use of third-party technologies, application programming interfaces (APIs) and complex applications have all increased the potential entry points available to cybercriminals. For this reason, the battle that fintechs face in securing their data against cybercriminals will always weigh in the attacker's favour. An attacker has to find just one major vulnerability among all the technologies in play to initiate a devastating data breach.

Aggressive growth outpacing security

Securing your IT estate is a bit like plate-spinning. It can start off manageable but, as more objects are added, it can quickly spiral into a frantic attempt to keep everything from toppling. In reality, fast-scaling fintechs are often rapidly adapting to their growing size and this can lead to the emergence of new security issues and exacerbate existing ones.

For smaller firms, the lack of dedicated security resources can lead to poor security hygiene. And it's this security shortfall that is utilised by attackers to compromise a business. The attempted ransomware attack on Finastra last year is a perfect example of this. Budding fintechs need to continually invest the right level of resources maintaining basic security practices throughout the scale-up process. This should naturally reduce the prevalence of common security headaches as they grow larger.

Balancing security and convenience

Fintechs have challenged banking goliaths by offering consumers what they want, when they want it and by removing friction. Challenger banks, such as Atom and Starling, have worked hard to improve the onboarding process in particular, using facial recognition software to streamline the process. And, while few will argue that fintechs shouldn't use innovative technology, they must stay abreast of evolving threats.

Within the realm of biometrics, artificial intelligence is becoming increasingly sophisticated in the way it mimics typical biometric indicators. For years cybercriminals have attempted to use photos and pre-recorded video footage to bypass challenger bank biometric-based verification systems. But with advent of deepfake technology, it is becoming difficult, even with human inspection, to determine a fake from the genuine individual. Fintechs may find themselves having to walk the fine line between providing convenience and maintaining security as threats continue to evolve.

Reliance on third-party integrations

Most fintechs would find it rather impossible to avoid integrating third-party APIs into their offering. Integrating APIs can deliver rich and seamless customer experiences, but being mindful of where they share customer data and what access they provide to third parties is critical.

Last year, the personal data of 7.5 million users was exposed when third-party service Waydev, used by US challenger

Account details alongside personal data are just two examples of the juicy information attackers are looking to sink their teeth into

bank Dave, suffered a breach. Usernames, emails, physical addresses, dates of birth and phone numbers were all stolen. With trust and reputation so critical for most fintechs, vetting third-party stakeholders and ensuring that they are taking necessary security precautions to safeguard data really does matter.

Remote working teething issues

As a consequence of the pandemic, most fintechs have had to adapt to a remote working setup for staff. This shift in working practices has created a new wave of security challenges, including ineffective device administration, increased susceptibility of staff to social engineering attacks and the introduction of vulnerable home networks.

Attackers have also had to adapt and they've become increasingly creative and successful. The growth of business email compromise attacks is one way that attackers have used the disruption caused by Covid-19 to their advantage. The shortcomings around promoting cybersecurity awareness and providing staff training to highlight the threats when working from home has also been notable. This has led to remote workers emerging as ripe targets for exploitation.

Fintechs have done a relatively good job of safeguarding their users' data thus far. However, what is certain is that they all face an increasingly hostile digital world, with an increase in both basic and more sophisticated attacks set to test them in the year ahead. Which firms will successfully navigate the challenge? TFT

About Predatech

Predatech was established to help businesses solve these challenges. We do this by helping clients to discover and remediate weaknesses in their security posture and promoting security best practices. We offer a range of testing services, from vulnerability assessments to penetration testing and tailor our services to meet your specific needs. Our mission is to make security testing accessible to all UK businesses, no matter their size, and to help turn the tide against the growing cyber threat.

Website: www.predatech.co.uk

LinkedIn: www.linkedin.com/company/predatech

Twitter: @PredatechSec

Predatech

TURNING TO SAAS TO SECURE DIGITAL FINANCIAL SERVICES

Thomas Bachman, Chief Information Security Officer, Mambu

Passionate about finding solutions for increased security challenges in the evolving fintech landscape, we discuss the ways in which a modern software as a service (SaaS) cloud banking platform can bring business agility and allow for easier integrations, all while maintaining the high security requirements for regulated financial institutions.

Kickstarted by a wave of transformative digital innovation, the last decade has experienced the most rapid evolutionary change yet in global banking. While the move to digital banking was already well underway prior to Covid-19, the crisis has accelerated this shift· forcing more people to move to digital channels and businesses to embrace the necessity of modernisation.

However, many financial institutions continue to struggle to meet these demands and are held back by their legacy systems, which don't allow for easy integrations. In turn this requires much more effort, time to market and cost to implement secure integrations, compared to modern systems that can provide these capabilities 'out of the box'.

Evolving customer preferences around how they interact with their financial institutions has pushed the digital channel to the forefront. This has helped better serve the industry through things like modern SaaS cloud banking platforms.

EVOLVING IN A SECURE ENVIRONMENT

Historically, banks were hesitant to adopt cloud technology because of a misconception that cloud (the public c loud in particular) is unsecure. While this misconception has fallen by the wayside, banks are still proceeding with caution. Even financial regulators are evolving and increasingly embracing cloud technology.

In selecting a SaaS solution, the provider offers the bank innovative and secure technology that can help alleviate the burden of securely hosting and maintaining such critical systems by the IT department of the bank. Instead, the provider, who knows the system best, can apply economies of scale for hosting, maintenance and implementation of security controls across all customers. This can be performed significantly more efficiently and therefore leave extra capacity to invest in stronger security measures, stability, as well as functionality of the solution. This allows institutions to keep pace with the evolving landscape while at the same time reducing operational risk for the bank and breaking them free from cumbersome legacy systems.

Banks operate in a highly regulated and sensitive environment and want to be reassured that the SaaS vendors and cloud infrastructure providers they work with are making security as much of a priority as they are themselves.

INNOVATING SECURELY IN THE CLOUD

The unmatched pace of digital change is pressuring banks and financial services providers of all sizes to accelerate innovation and increase their agility. The desire to achieve greater business agility through flexibility and scalability is also a driving factor at play here. Yet as banks and financial services providers migrate to the cloud, security and compliance are priority considerations.

SaaS banking platforms that support composable API-enabled architectures allow banking and financial institutions to operate like technology companies. Working with providers like Mambu enables firms to scale their core banking business in the cloud and empowers them to innovate faster while operating in a secure and compliant environment. The cloud enables businesses to lower their costs, bring new ideas to market at a competitive pace, and create more streamlined and personalised customer experiences. This can all be done while meeting strict security compliance and regulatory requirements.

TURNING TO SAAS FOR TRUSTED DIGITAL SECURITY

Cloud providers today are held to high security standards, which means these digital environments are equally, if not more, secure than on premise solutions and provide the opportune setting in which businesses can launch and scale at pace. In addition, the flexibility of the cloud allows technology providers to support banks and financial services firms in addressing a wider client base. This can result in driving access to transformational technologies available primarily through the cloud or by speeding up time to market for new financial products.

There are many important security issues and best practices that banks must consider when transferring regulatory compliance systems and processes to SaaS solutions. But first and foremost, it's important for businesses to take a step back and evaluate if they are being proactive in their efforts towards meeting their customers efficiently, effectively and securely on the digital channel· And, if they aren't, they need to reprioritise in order to future-proof and address their customers' demands for a more digital and secure approach. TFT

JOBS IN FINTECH

The Fintech Times selection of TOP fintech jobs this month

Head of Product Design at CURVE

Curve was founded with a rebellious spirit and a lofty vision; to truly simplify your finances so you can focus on what matters most in life. That's why Curve puts your finances simply at your fingertips, so you can make smart choices on how to spend, send, see and save your money. We help you control your financial life, so you can go out and live the life you want to live.

ROLE PURPOSE:

We're looking for a talented Head of Product Design to join our core product function at the heart of our London HQ. If you you're passionate about solving real problems for real people and you love what you do, then this job is for you.

As a Head of Product Design, you will lead Curve's Product Design function, shaping and moulding them into an elite team of problem solvers they strive to release new products and functionality to our customer base across the globe. You'll also be a primary contributor to our overall product vision and strategy in collaboration with our Head of Product, as well as other key stakeholders. In addition to this, you'll also be actively contributing to the betterment of product and design lead strategy and thinking, and disseminating this methodology across the wider company.

KEY ACCOUNTABILITIES:

- Hiring great designers at scale, helping them to succeed and grow through close mentorship and collaboration
- Driving the design function forward by developing new ways of working and improving design systems
- Disseminating design thinking throughout all areas of the business, and contributing to our product and design-lead strategy and culture.
- Improving implementation and release processes with various stakeholders, such as product, engineering and data leads

THE REQUIREMENTS:

- Have 8+ years experience as a designer who has delivered ground breaking digital products as an individual contributor
- Have 3+ years experience as a design manager, leading and mentoring designers
- Are an expert collaborator, with a great knowledge of data, engineering and product principles
- Are a promoter of customer centricity, seeking to always delight customers through a data driven approach
- Have experience developing, maintaining and upholding proper usage of complex design systems for both mobile and web products

Vice President of Product at onfido

Onfido is the new identity standard for the internet. That means we only need an image of your ID and a selfie to prove that you're you. In doing so, we help millions of people connect to the services they need and love more easily, speedily and safely than ever before, whether it's renting a car or opening a bank account. Our vision is to create an open world where identity is the key to access.

As the Vice President of Product Management reporting to the Chief Product Officer, you will play a key role in providing end-to-end ownership of Onfido's core product lines to help build a world class product portfolio and grow each product line to support Onfido's mission to be the market leader in identity verification and expand our product offering with new products.

THE REQUIREMENTS

- Have previously served as a VP Product (or related position in larger firm) in a similar-size company or product line
- Must be able to build strong trusted scaleable relationships with the various corporate stakeholders, and in particular with R&D, growth, and marketing
- Able to demonstrate successful deployments of prioritisation frameworks across a global product platform
- Demonstrated ability to teach and coach the product management skills across the full product lifecycle. A successful candidate should have past direct report examples demonstrating successful development and mentoring of high performance individuals
- Have the technical depth to understand our technological challenges and lead meaningful conversations with engineering and research. A degree in CS or a related field would be a plus
- As a plus, have experience working with a high-calibre research team that can help drive product agenda via innovation

THE BENEFITS

We're committed to making Onfido a fantastic place to work, so we go to great lengths to give you what you need to succeed. You'll receive:

- Share options in Onfido, through our equity schemes. Share options have a one year cliff and start vesting after probation over a four year period*
- Bupa Private Medical and Dental Insurance*
- Life Assurance (3x Annual Base Salary)*
- Pension with The People's Pension (employer contribution four per cent of base salary)*
- Generous paid parental leave
- Free mental health coaching provided online.
- Life enrichment allowance of up to £80 per month to use for services

Fullstack Developer at YAPILY

Yapily is here to power a new era of financial services so that everyone can receive faster, affordable and personalised products. Yapily uses an open API, powering applications behind the scenes, to seamlessly connect and securely access financial information. We enable companies to access financial information to enrich the customer experience in Banking, Lending, Payments, Accounting and Money Management.

In April 2020, we raised $13m in Series A funding, this is an incredibly exciting time to join the business as we begin to look towards launching internationally and are building the marketing team from the ground up, with huge scope for autonomy and influence.

We are looking for Java Full Stack developers who have also knowledge and passion for frontend and UX development. For this position, we are looking for candidates with a strong background in OO design with Java and at least one other programming language, experience working with web services, Spring Boot and core frontend CSS, HTML, JavaScript. We use different technologies for different frontend applications, some using the Vaadin framework for full Java stack, others with Vue and Node, and also React or Flutter for native apps.

Equally important to these specific skills is the ability to multi-task, quickly adapt to new development environments and changing business requirements, learn new systems, create reliable/maintainable code, and find creative and scalable solutions to difficult problems.

YOUR RESPONSIBILITIES

- Support, maintain and build customer-facing applications, that can be web or mobile applications
- Build API clients to consume data from multiple sources, normalising and aggregating formats, in real-time or distributed reactive streams
- Manage individual project priorities, deadlines, and deliverables

THE REQUIREMENTS

- BA/BS degree in Computer Science or equivalent technical work experience
- Strong Computer Science fundamentals
- 3+ years of development experience
- Outstanding knowledge of Java
- Able to bring experience and ideas that will help Yapily deliver highly efficient and reliable services

THE DESIRABLE

- Spring Boot framework
- One of these would be great: Vaadin, Android Java, Android Kotlin, Flutter, web frameworks

THE FINTECH POWER 50
KICKSTART
TALENT IN FINTECH
SHAPE A NEW FINTECH FUTURE
YOUR CHANCE TO HIRE YOUNG PEOPLE, FULLY FUNDED
FinTech Wales
EPA EMERGING PAYMENTS ASSOCIATION
INNOVATE | FINANCE
L39
iFinance ACADEMY
PART OF THE CONEXUS GROUP
JOBBIO
rise
Created by BARCLAYS
THE FINTECH TIMES

AIBC
ASIA
MANILA
27-28 MAY 21

DOING DIGITAL

George Baily, Marketing Manager, CREALOGIX

"Two years ago, people talked... last year, they were still talking... This year, they are still talking... The question is: show me what you are doing here? Show me your work... show me results," said Chen Long, chief strategist at Ant Financial, in an interview in Chris Skinner's last book, *Digital Human* (2018). In Chris's new book, *Doing Digital,* he tackles this question of talk versus action in a strongly worded critique of the state of transformation and strategy in our industry.

While *Digital Human* took a wide-angle view of 'a revolution of humanity through digitalisation with technology, *Doing Digital* adjusts the lens to examine the idiosyncratic world of banking. In fact, in this book it often feels like a magnifying glass is being held in the sun so as to burn a hole in an industry that clearly frustrates the author with its complacency and slow rate of change, despite being besieged by obvious and massive competitive forces.

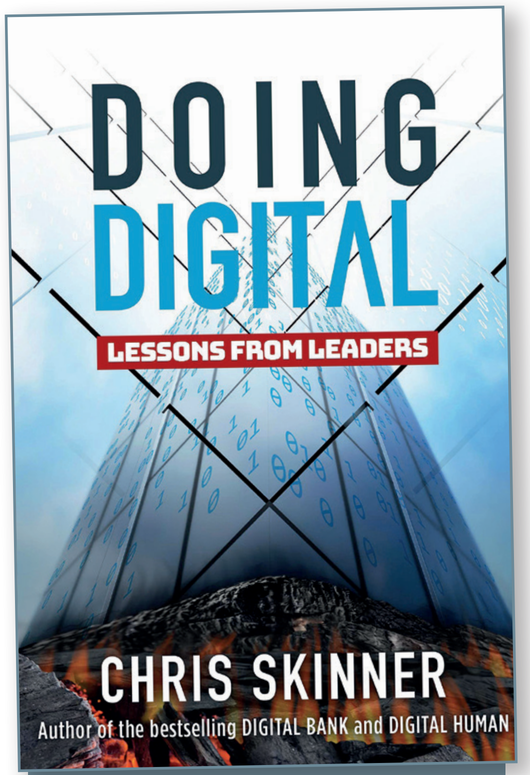
Outlining the competitive pressures from fintechs, challengers, big tech, regulation and internal inertia, Chris calls for 'drastic action, not an evolution' – and woe to anyone trying to get away with half measures: 'any bank that has not embraced digital as a transformational process, but just as an evolutionary process, will sleepwalk into history'. As you can tell, Chris does not hold back – the book is packed with pithy indictments of the state of the industry: 'the business model of the banking industry is completely broken' and 'we need to rip that structure apart'.

Change in the industry is too often reactive: 'banks do change, but most of it is stimulated by fear'. In Chris's view, change must be strategic and proactive. Instead of being primarily led by the moves of regulators, competitors, or even their investors, banks should organise around a greater respect for their customers: 'technology and digital change... is about customers and service. Technology has placed the customer in control'.

As this point about customer-centricity illustrates, despite his harsh words about banking leadership, in this book Chris sets out a positive, even idealistic call to action, including several sections organised like checklists, e.g. 'seven new ways in which finance delivered by technology is changing the game', 'five areas of change'...'five clear areas that are forcing transformation'. The strongest sections of the book take aim at common corporate excuses, countered in a highly critical but also highly optimistic voice that will be familiar to readers of Chris's blog The Finanser.

Chris quotes from a variety of industry leaders whom he feels are setting a good example: in fact, he considers there to be – 'a mere nine large banks worldwide that I thought were making digital transformation happen'! Their success stories are contrasted with the all too common scenario of overspend and bureaucratic activity that fails to deliver.

Pure technology competitors do have an obvious head start: 'if a bank is just sticking apps on the front end, how is it meant to keep up with its competitors' deep learning projects?' Fintechs are unburdened by any technological legacy, whereas banks are too often 'firmly rooted in last-century technologies'. Old technology creates its own vicious cycles. Readers who work within large financial institutions will no doubt read with a mixture of despair and amusement how 'a big bank will often waste 20 to 30 per cent of its investments on internal politics', and if they are themselves change advocates will likely recognise this analogy for organisational resistance: 'innovation was like a virus that had entered the organisation and challenged it. As with any virus, the white blood cells soon gathered to squeeze it out'! Technology work in the 'spaghetti bank' is thus unrewarding, while 'the innovators are already a mile down the road of taking out the banking system as we know it'.



Doing Digital: Lessons From Leaders *by Chris Skinner is published by Marshall Cavendish International (Asia) Pte Ltd*
Available: Kindle, Hardcover

And that, Chris explains, is the more fundamental issue than any specific technological change: the necessity to throw out a business model designed around banks and paper. Throughout this book we are reminded how the strengths of the past can hardly be relied on to take financial institutions into the future ahead: 'banks have plenty of legacy: legacy systems, legacy vendors, legacy staff, legacy customers, and, worst of all, legacy leadership'. The answer in this book is to address the latter, with Chris pulling no punches: 'most banks are led by bankers... with no technology experience or digital background' and 'dealing with technology is very different to dealing with money'.

Using wide-ranging examples of innovation both from digitally-native startups and Chinese 'techfin', as well as the more progressive incumbents, Chris emphasises the existential challenge old-fashioned banks face: 'in five years, banks will make no money from what they do today and will need to be competitive in [a] new, proactive, augmented world.'

With such an urgent challenge, it's perhaps counter-intuitive to find that Chris asserts that leaders in financial institutions need 'room to breathe'. A key observation arising from Chris's look at digital success stories is that attempting major institution-wide change is not something achieved with normal management horizons but a longer view.

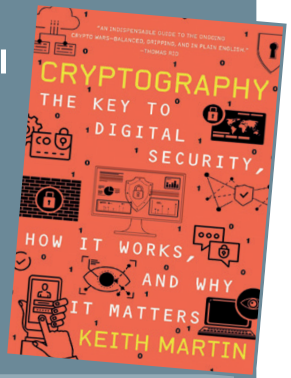
Shareholders themselves need to take a longer view: 'protecting the leadership of the bank from worrying about those financials and giving them the mandate to focus on the change'. So, in one sense, boards being too risk averse about change in the digital era could prove to be the riskiest strategy. The world of banks 'is built around maximum stability and minimal change. That is not a good recipe for digital transformation'.

Chris gets to the heart of the matter when commenting: 'there is a huge difference between 'doing digital' and 'being digital' – the question being, can the incumbents change who they are, in order to revolutionise what they do?

This means, the book title notwithstanding, that 'doing digital' is really the outcome of a more fundamental change of raison d'être, rather than superficially seeing how much technology the organisation can adopt. As Chris explains: "It is a book about change. How to make dramatic change happen... how to turn an age-old institution into one that is nimble and refreshed for the digital age... how to make the elephant dance." This image is certainly a more positive alternative to the two more common elephant metaphors I hear in conferences: eating elephants one bite at a time or there being elephants in the room. The real question is... 'whether banks have recognised the real need to change'. Chris's polemic book suggests that the answer is still too often 'no'. If you work in fintech, particularly within or alongside incumbent institutions, buy two copies – one for the boss's desk and the other for yourself to help 'deal with the revolution'. TFT

5 BOOKS TO GET AHEAD IN FINTECH

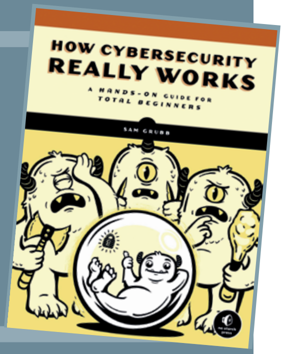
Cryptography: The Key to Digital Security, How It Works, and Why It Matters *by Keith Martin*
Available: Kindle, Audiobook, Paperback and Hardcover


CRYPTOGRAPHY
THE KEY TO DIGITAL SECURITY,
HOW IT WORKS, AND WHY IT MATTERS
KEITH MARTIN

Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity *by Hamid Jahankhani, Stefan Kendzierskyj, Jaime Ibarra and Nishan Chelvachandran*
Available: Kindle and Hardcover (7 April)

Advanced Sciences and Technologies for Security Applications
Hamid Jahankhani
Stefan Kendzierskyj
Nishan Chelvachandran
Jaime Ibarra Editors
Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity
Springer

Cybersecurity for Beginners: A Hands-On Guide *by Sam Grubb*
Available: Kindle and Paperback


HOW CYBERSECURITY REALLY WORKS
A HANDS-ON GUIDE FOR TOTAL BEGINNERS
SAM GRUBB

Safe Banking & Trading: Home banking and online trading security *by Antonio Luben*
Available: Kindle Edition

Reinventing Banking and Finance: Frameworks to Navigate Global Fintech Innovation *by Helene Panzarino and Alessandro Hatami*
Available: Kindle, Paperback and Hardcover

Helene Panzarino and Alessandro Hatami
REINVENTING BANKING AND FINANCE
Frameworks to navigate global fintech innovation

THE FINTECH POWER 50

WOULD LIKE TO THANK ALL OF ITS SPONSORS, PARTNERS AND INFLUENCERS

THEODORA LAU

JIM MAROUS

CHRIS SKINNER

BRETT KING

DEVIE MOHAN

DAVID BIRCH

GHELA BOSKOVICH

LAWRENCE WINTERMEYER

RUTH WANDHÖFER

DAVID PARKER

rise Created by BARCLAYS · METRO BANK · DLA PIPER · EPA EMERGING PAYMENTS ASSOCIATION · THE FINTECH TIMES

FINTECH SANDPIT · THE ASIAN BANKER STRATEGIC BUSINESS INTELLIGENCE FOR ASIA'S FINANCIAL SERVICES COMMUNITY · SkyParlour

JUMIO · Funding Options · Contis · EMQ · SmartStream · PENGUIN PORTALS · boss INSIGHTS · SERRALA

BANKING CIRCLE · modularbank · novastone · OakNorth · FORM3 FINANCIAL CLOUD · CREALOGIX

IDnow · Grab · bud · OpenPayd UNLOCKS BANKING · Flybits · Konsentus · Currencycloud

W2 · tide · OneConnect Financial Technology Co., Ltd. · nanopay · meniga · token · Bottomline

SALTEDGE · SPHONIC · GPS global processing services · wesure · FINGOPAY · Wing

GALILEO · Keepabl™ · BANKIFI · RESPONSIVE · OMNIO · Bankable