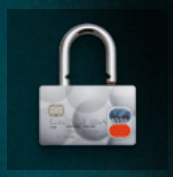
FUTURING PAYMENTS

A WORLDLINE MAGAZINE | OCTOBER 2020 | EDITION #3

2020: A MOST UNUSUAL YEAR

Interview with **Gilles Grapinet**, Worldline CEO



LATEST TRENDS IN SECURITY AND FRAUD RISK MANAGEMENT

- Inside the Mind of a Hacker
- Trends in Global Payment Fraud
- The World Map of Fraud

STABLECOINS

- Stablecoins - Next Generation Regulated Digital Currencies
- The DaVinci Gold Token

DIGITAL PAYMENTS FOR A TRUSTED WORLD

Worldline

TABLE OF CONTENTS

LATEST TRENDS IN SECURITY AND FRAUD RISK MANAGEMENT

STABLECOINS

WELCOME TO FUTURING PAYMENTS EDITION #3

Pascal Mauzé,
Head of Sales & Marketing at Worldline

The year 2020 will go down in history as the year of the COVID-19 pandemic.

This third edition of Futuring Payments begins with an in-depth interview with Gilles Grapinet, CEO of Worldline, in which he analyses the COVID-19 situation seen both from a payment industry perspective and from a more personal perspective as a leader of thousands of people in a large international company. The pandemic is first and foremost a global catastrophe, but there are also bright spots that we should pay attention to. The pandemic has forced us to think alternatively in several situations, and if we act wisely, something positive can come out of it as well.

In the interview, Gilles Grapinet also talks about his expectations for Worldline's acquisition of Ingenico, which is now becoming a reality. He also shares his views on the current status on fraud in the payment industry, which is the central theme of this edition of Futuring Payment.

Fraud is one of the most critical and resource-demanding challenges in the payments industry today for issuers, acquirers, merchants and consumers. Effective fraud prevention and fraud monitoring is crucial to maintain the trust needed to run local and global payment systems. At the same time, criminals are becoming more and more sophisticated, and often the most successful attacks are executed by highly skilled, international criminal organisations around the world.

In this issue of Futuring Payments, we analyse payment fraud from several angles. We look at the topic both from the hacker's viewpoint and from the view of the payment industry professionals working day in and day out to neutralise and eliminate criminal activity. And we interview a number of experts about how fraud within the payment industry is likely to develop in the future and ask about their advice on how to fight it efficiently.

The good news is that the different parties in the payments industry, even though they are fierce competitors, are joining forces to fight fraud and cybercrime through international forums and organisations like for instance the ECRB under the auspices of the European Central Bank (ECB). These collaborations are increasingly giving cause for optimism in the fight against fraud.

This edition of the magazine also introduces our readers to the fascinating topic of stablecoins. Worldline is at the forefront of helping its clients utilise the potential of blockchain technology, and we explain how we have been collaborating to develop DaVinci Tokens which are blockchain-based tokens backed by gold.

Happy reading and see you again soon!

2020: A MOST UNUSUAL YEAR

INTERVIEW WITH **GILLES GRAPINET**, CHAIRMAN AND CEO OF WORLDLINE

Gilles Grapinet,
CEO, Worldline

In this comprehensive interview, Gilles Grapinet looks back on some of the most important issues of 2020, a year of severe challenges and also of more positive developments.

First and foremost, 2020 has been an extremely unusual year due to COVID-19. The initial topic of this interview is the consequences of the pandemic as seen from a payment industry point of view. Despite the catastrophic implications for health and for the global economy, there are some positives that have emerged during the crisis, not least when it comes to digitisation and the reduced use of cash.

The second topic is cybercrime and fraud, an issue which for some time has been moving higher and higher up the agenda of the payments industry. How to build strong defences and manage every shade of fraud is the central theme of the current issue of Futuring Payments and is also addressed in this interview.

Finally, 2020 has been a very special year for Worldline because of the acquisition of Ingenico, one of the leading payment companies in Europe. In this interview, Gilles Grapinet discusses the motives behind the acquisition, outlining his vision of the new Worldline and explaining why he considers Worldline and Ingenico to be a perfect match.

COVID-19: IDENTIFYING THE GREEN SHOOTS OF RECOVERY

The current pandemic is first of all a catastrophe for people, companies and countries all over the world. But in the gloom there are some encouraging developments. The crisis is teaching us new lessons, showing us new ways of operating and highlighting the huge potential of digitisation. Gilles Grapinet singles out some of the positive consequences for the payments industry.

Question: In May, Worldline published a whitepaper on the consequences of COVID-19. The report pointed out an increased digitisation in businesses and society, an acceleration of cashless payments, a boom in online retail and an increasing demand for omnichannel experiences. Now, five months later, do you see the first signs of these new trends?

Gilles Grapinet: We are currently witnessing the materialisation of the early observations and forecasts that we made in May. COVID-19 has had a transformational impact on the way people behave in the most affected countries. And within our industry, the consequences encompass both digital payments and e-commerce. Even though the majority of physical shops have come back into operation after weeks or even months of lockdown, we still see very strong momentum for e-payments in general.

> If things continue to develop the way they currently are, we will probably have gained two or three years in terms of the market share penetration of contactless payments, card payments and online commerce, at least in Europe, and maybe even more in certain countries

The same goes for the omnichannel experience, because when e-commerce accelerates the need increases for merchants – even the ones with large store networks – to offer a much more unified customer experience. Online and physical shopping are converging to the benefit of the customer. Furthermore, since the outbreak of COVID-19, we have seen a substantial increase in contactless payments – with limits extended to €50 without the need to apply a PIN code – in physical shops.

So even though COVID-19 is a global crisis in many ways, there are some aspects that could be turned into positives?

Gilles Grapinet: First and foremost, these are specific observations carried out by payment specialists. But we must never forget that ultimately the COVID-19 black swan event is a catastrophe for our societies and for humankind. It has significant macroeconomic consequences, including potentially a massive increase in unemployment for millions of people, and already a loss of more than one million lives.

Nevertheless, it is reassuring to see the impressive resilience of our societies and of companies in general. The way we were able to adapt very quickly to remote working at scale is unprecedented. Ultimately, we have been able to maintain the normal functioning of our societies during extraordinary circumstances.

Our adaptability, both individually and collectively, was remarkable. For instance, payments adapted very rapidly. With scientific studies indicating that the COVID-19 virus can survive on surfaces, including cash, authorities swiftly communicated this information and merchants and customers quickly embraced a shift to contactless, electronic payments. It all happened extremely fast, driven by unprecedented public concerns about transmission of COVID-19.

Also, banks and key stakeholders immediately increased contactless thresholds. And merchants and customers immediately adopted new behaviours and increasingly started to do their shopping by using online channels.

I think we can all be proud of this ability to adapt to a new reality. And what we are doing now is trying to take advantage of this transformation, to help rebuild growth and to recover part of what has been lost.

Has the COVID-19 crisis in some ways changed a lot of companies forever? For instance, their CSR strategies or their way of working together?

Gilles Grapinet: This crisis reminds all of us that the way we take care of each other as individuals, and the way we take care of our companies, really matters.

As a company, our first duty at Worldline was to protect immediately our people as much as possible, and to adapt our ways of working to the unprecedented COVID-19 circumstances, while at the same time making sure that we were delivering flawlessly on all contracts to thousands of merchants and key customers across the world.

We needed to be able to keep a high level of interaction with our people in order to maintain the ongoing initiatives and projects and essential elements of development for the company in a virtual working situation. And we needed all employees to feel that they still belonged to the community of the company while at the same time protecting their health by staying at home and making sure they do not contribute to the spread of the virus. All in all, the situation was highly critical and complex, but we were able to manage it well and our strong commitment to corporate social responsibility was more important than ever and made it possible to connect all the dots.

FRAUD: AN INDUSTRY WORKING TOGETHER TO OUTSMART THE CRIMINALS

In the past and right up to the present day, fraud has been a serious challenge for the payments industry. However, Gilles Grapinet has an optimistic view of the fight against cybercrime and fraud. He sees a strong payments industry coming together and resisting attack more efficiently than ever before.

The central theme of this issue of Futuring Payments is fraud and risk management. In a recent analysis, Worldline estimates that total online payment fraud this year will be at least $25 billion. In your opinion, how significant a threat is fraud for the ongoing and further digitisation of payments and the development towards a society with less cash?

Gilles Grapinet: If we look at fraud trends, in the past we have been able to manage fraud relatively efficiently by continually improving our defence systems. Fraud has always been part of the history of payments. When payments went electronic, it only took a short while before we saw the first attempts to hack and commit fraud in the new systems. It is an ongoing technology race between the criminals and the payment industry, but Europe has taken probably one of the most advanced and progressive stances against electronic payment fraud by being an early adopter, in particular, of chip & pin technology. And this has immensely reduced the level of fraud associated with debit and credit cards. PSD2 and the mandatory strong authentication implementation for card present transactions is also a proof of willingness in Europe to minimise constantly the level of fraud.

The main challenge is always the same: to gain maximum efficiency in the race against fraud on the one hand, while not creating unnecessary friction for the customer on the other hand.

> So, striking the right balance between security and convenience on the payment journey is continuously at the centre of what we do.

If fraud increases and convenience goes down due to increased security, do you see a risk that we will scare users away from digital payments and back to cash?

Gilles Grapinet: I don't believe so – for multiple reasons. Firstly, at Worldline, it is very important for us to help merchants ensure that they are dealing with legitimate customers making legitimate transactions. And at the same time, reassuring consumers that they are protected when using electronic payment solutions. The way we protect transactions, and the way we detect fraudulent patterns and abnormal use of the payment infrastructure, need nonetheless to be as invisible and as fluid as possible.

But the fact that we care so much helps us to build trust. I don't mind being regularly asked to confirm on my smartphone that I am actually carrying out an online transaction from my laptop. On the contrary, it strengthens my trust in the system. And trust in payment is at the root of everything we can do!

We have reduced the level of fraud very efficiently over the past ten years, particularly within online payments. And this has helped to keep e-commerce growing firmly and steadily. Year-on-year, customers' and merchants' trust in the management of the payment systems is increasing. We need to upgrade the systems constantly, but all in all, things are developing in the right direction.

Also, the industry is still a long way from using the full potential of new and innovative technologies to make electronic payments easier and safer for end-users. For example, we have not yet utilised the possibility of implementing advanced biometric systems on a large scale. All this is still a largely untapped potential.

One way of fighting fraud and cybercrime is through the sharing of information across countries, sectors and companies, which makes it possible to build more robust defences. The Euro Cyber Resilience Board (ECRB) of the ECB and the European Digital Payments Industry Alliance, EDPIA, are examples of this. How would you describe the value of working together and sharing information – even amongst competitors?

Gilles Grapinet: Fraud is like global warming. It is a common global challenge. Most of the time, when it comes to really sophisticated fraud, we are talking about organised crime.

So, fundamentally, we have a genuine interest in sharing knowledge and information, in collaboration across the industry, and in contributing to working groups in particular with public stakeholders and regulators.

Standardisation in the industry is always beneficial. Competitors working together to increase the level of standardisation is not problematic. On the contrary: it is desirable. For instance, within EDPIA, we are gathering the largest industry players in Europe, and we intend to participate in European working groups where fraud will be a topic to be jointly addressed. We are all in the same boat here.

WORLDLINE AND INGENICO – A PERFECT MATCH

Worldline has acquired Ingenico and is now by far the largest payment company in Europe. But Gilles Grapinet says this is no reason to sit back and take it easy. Worldline is still a young company, the journey has only just begun, and there is a greater vision waiting to be realised.

Finally, let's talk about Worldline's recent acquisition of Ingenico, making Worldline Europe's new world-class leader in payment services. Does this acquisition make you feel proud?

Gilles Grapinet: Worldline is still a young company. Yes, we have existed for decades, but most of the time as a part of Atos Group. As an independent, listed company, we are still pretty young. We were listed in 2014 and we became independent only last year, in 2019.

To answer your question: it is not at all the time for us to be proud of anything! We are still at the start of our journey. We are in motion, in action, we are in the heat of the transaction and our focus is on the best possible integration of Ingenico. So, the only thing that is really meaningful for us right now – and I believe this is just as true for Ingenico as it is for Worldline – is that we have a joint vision that we can realise in Europe, from Europe and in a certain sense for Europe.

We want to be a European industry player of global scale, and we believe that we have a significant role to play in the future. The acquisition of Ingenico is a highly strategic move for Worldline.

> And in a post-COVID-19 world, to continue building European players of scale that can ensure European competitiveness, whether it is in pharmaceutical products, semiconductors, or electronic payments, is more meaningful than ever.

I am happy to see that the markets are supporting the acquisition. It will triple our exposure to e-commerce and online payments. It will massively expand our position, particularly in the Nordic countries. And it will give Worldline a leading position in Germany, the largest European economy, where Worldline was smaller than Ingenico.

Worldline will also reinforce its geographic position in Central and Western Europe. We will get the benefit of massive scale and the capacity to double our investments in terms of R&D and innovation. Finally, and most importantly, we are about to increase the company by welcoming 8,000 new Ingenico payments experts from all over the world. And we are very eager to start operating as one company.

As a Worldline client, will there be benefits for me or my customers because of the Ingenico acquisition?

Gilles Grapinet: Fundamentally, what Worldline can offer is unique, because we have an exceptional reach and presence throughout Europe. Whoever you are, and wherever you, as a merchant or a bank, are located in Europe, Worldline is the company speaking your language, living next door to you, bringing you in one value proposition unmatched industrial scale, leading-edge innovation for online and offline payments and, just as importantly, local and cultural intimacy combined with pan-European presence and global reach.

With the Ingenico acquisition, we are at the same time gaining a significantly stronger global reach beyond Europe, enabling us to also serve clients in Asia, and Latin America, and even in the US. I believe that over time this will make Worldline fully live up to its name and its visionary brand adopted long ago, as we want to contribute more and more to connect banks, businesses and commerce with their customers all over the world, for their smart, secured and frictionless payments. It is an incredibly motivating project for everyone in our company to pursue building together a new global brand in digital payments!

PREPARE FOR THE POST-COVID-19 WORLD

A new report by Worldline helps companies and decision-makers prepare for the state of the world now and in the aftermath of the COVID-19 pandemic. Read a summary of the whitepaper here and follow the link below for a download of the full text.

For a global company like Worldline, there are many good reasons for actively monitoring the development and the consequences of the COVID-19 crisis. We have employees, clients and partners all over the world that we care deeply about. We play an active role in numerous countries and societies where our business is present. And the industry that we are part of happens to be one that will play an essential role in the aftermath of the pandemic – underlined by the fact that the crisis has shown a clear need for a significant acceleration of global cashlessness and digitisation in general.

In the report, Worldline looks at impacts for both society and businesses, immediate as well as lasting.

IMMEDIATE IMPACTS

Immediate impacts for societies as well as for businesses around the world include essential digitisation, the acceleration of cashless payments, and a rise in online retail and omnichannel.

ESSENTIAL DIGITISATION

The most immediate impact for companies is what Worldline calls essential digitisation, which is about companies replacing as much as possible physical services and in-person ways of working with virtual equivalents. During periods of lockdown, many companies had an immediate need for efficient software tools in order to stay operational while employees are working from home. But the increased use of multiple communication platforms and tools like SMS, WhatsApp, Skype, Zoom, Microsoft Teams, Webex, etc. also raises new security challenges for many companies.

CASHLESS ECONOMY

Another area close to the heart of Worldline that has seen a massive acceleration as a direct consequence of COVID-19 is the movement away from cash. Coins and notes are not only expensive for societies, inefficient and supportive of criminal activities; they are also contaminated with lots of bacteria, and potentially able to transmit viruses. The replacement of cash payments with a variety of digital payment solutions including contactless cards and mobile payments has of course been going on for several years, but COVID-19 has massively boosted this development.

In most regions the maximum threshold allowed for contactless payments has been raised, and MasterCard reported a 40% global increase in contactless usage worldwide in the first quarter of 2020.[1]

RISE IN OMNICHANNEL

Enabling the seamless customer journey transiting between various information and sales channels – called omnichannel – has been a key development in the retail space of the past years. However, the COVID-19 crisis made it crystal clear for many merchants that they desperately needed to be much more visible and accessible through online channels and not only in the physical world. We see that omnichannel models (like drive-in, click-and-collect) are becoming the default, even for small businesses. And for many companies, the urgent need to provide a seamless omnichannel experience with a more contextual and personalised service (from order placement through to collection/delivery) will be a new challenge.

LASTING IMPACTS

When it comes to the lasting impacts for companies, the report points to a new resilience of supply chains and a sustained shift towards smarter ways of working.

NEW RESILIENCE

The crisis revealed the fragility of many existing supply chains: highly dependent on single suppliers and efficient distribution channels. Going forward, Worldline expects businesses to adapt their approach to:

- Adopt multi-sourcing models to reduce dependencies on single suppliers
- Increase the degree of local sourcing
- Increase inventory (reduction of Just-In-Time).

SMART WORKING

At Worldline, even with 97% of its staff switching to homeworking during the lockdown, the company remained fully operational. Worldline believes that for all businesses, this sudden change in ways of working will lead to longer-term shifts in attitudes.

Working remotely has increased the amount of autonomy people have in their work and the way they are managed: rather than judging people by whether or not they turn up for work, they are being measured instead on the results they deliver. Worldline characterises this as a shift from teleworking to smart working.

TO READ **THE WORLD AFTER COVID-19** IN ITS ENTIRETY, INCLUDING A LIST OF TECHNOLOGIES WITH ACCELERATED RELEVANCE AND 10 KEY TAKEAWAYS, PLEASE DOWNLOAD THE REPORT VIA THIS QR-CODE:

1 https://www.nfcw.com/2020/05/01/366386/mastercard-reports-40-growth-in-contactless-transaction-volumes/

LATEST TRENDS IN SECURITY AND FRAUD RISK MANAGEMENT

INSIDE THE MIND OF A HACKER

INTERVIEW WITH **KASPER BRANDT**, HEAD OF ATOS' WHITE HAT HACKER TEAM

For companies to prevent hostile hackers from successfully attacking them, they need to understand how hackers think and what they look for. Too many companies today seem to have forgotten this simple lesson. In this interview with Kasper Brandt, who is the head of Atos' dedicated team of extraordinary white hat hackers, we are invited to get a firsthand understanding of the mind of a hacker. When does the nerdy fascination with solving complex programmatic challenges turn into criminal activities?

What does the hierarchy of hackers look like? Is there still a cultural and ideological aspect to hacking? What is the difference between a hacker and a cracker? And how do companies defend themselves better going forward?

WHAT IS A BEAUTIFUL HACK, IF SUCH A THING EXISTS?

Well, I think it does. A beautiful hack is a hack where you have thoroughly analysed the context, considered all the technical variables and found a solution that not only works once but every time. The beauty of a hack comes from the preparatory analysis and the entire research work that precedes the hack itself. A beautiful hack is when you sneak through without anybody ever noticing that you have been there. The opposite is the dirty hacks where the attacker just smashes his or her way through a system.

OKAY, LET'S TAKE ONE STEP BACK AND TALK ABOUT SOME DEFINITIONS AND THE STORY OF HACKING. WHAT IS A HACKER, AND WHERE DOES THE TERM COME FROM?

The mainstream idea of a hacker is a sinister guy with a hoodie sitting in a basement somewhere trying his best to harm innocent people. However, for those of us who work professionally with these things, a hacker is someone who has achieved the highest level of technical skills.

If we go back in time and look at the original meaning of the word 'hacker' in the early 1960s, a hacker was someone who could take any difficult IT problem and solve it. The hackers were the most capable students, for example from MIT, and they quickly became popular. The hacker was the good guy, whereas the bad guy was originally the cracker who had malicious intent. But the original distinction between hacker and cracker got lost in translation over time.

Famous from the 1960s is The Model Train Club from MIT's Building 20, which was probably the first hacker group in the world. It was a group of students who were fond of model railroads, and the first hack they conducted was when they broke into the telephone system at MIT and designed a technical setup of their train lanes so that the switching system was guided by the calls being made in the telephone network. So they created a model railway that was dynamically controlled by user input.

WHEN DID THE ORIGINAL DISTINCTION BETWEEN HACKER AND CRACKER DISAPPEAR?

It is only during the past few decades that being a hacker has turned into something bad and today hacker has become an umbrella term for anyone doing anything bad with a computer. Except for the small groups of so-called ethical hackers or white hat hackers who have only good intentions and try to give the positive meaning back to the hacker concept. The bad ones are usually called black hat hackers.

HOW ORGANISED ARE THE CRIMINAL BLACK HAT HACKERS TODAY?

> The Internet has made cybercrime a global business with a complete crime chain. global business with a complete crime chain. Typically, the experts who steal people's credit card information and collect it in large databases are not the same as the ones who exploit the information. The experts put the data up for sale on online trading portals, and the information is then purchased by criminal groups who are willing to exploit the information for fraud.

Kasper Brandt,
Head Of Atos' White Hat Hacker Team

Cybercrime is well organised and in countries like Russia, China, India and North Korea, you can find huge scam centres, which are almost like factories. In some parts of the world, scamming is completely industrialised like any other business. Huge centres with hundreds of employees with a daily focus on scamming people out of their money. And for the people who work in such a place, it might be the only job they can get.

The more sophisticated it gets, the more malicious it is too because you have to be really clever and highly skilled to reach the level where you can actually make sophisticated hacker attacks – and such dedication shows that you put a lot of effort into malicious acts. Those at the top of the knowledge food chain are clearly taking the hacking approach as an intellectual challenge. And unfortunately, some of them end up crossing the line and start using their skills illegally.

DOES IT MAKE SENSE TODAY TO TALK ABOUT HACKER CULTURE AND A HACKER IDEOLOGY, OR IS IT RATHER AN INDUSTRY OR A SPORT? INITIALLY, PARTS OF THE HACKER ENVIRONMENT WERE LINKED QUITE CLOSELY TO ANARCHIST CYPHERPUNKS AND LIBERTARIAN TYPES.

In the vast majority of cases today, technical challenges unite the hackers and not an ideology or a culture. Today it's more of a technical sport. Of course, the hacker environment still has strong attitudes to surveillance and the like, but at least in the public forums, ideology no longer means much. So, it's no longer ideological ties that hold the community together.

DOES THAT MEAN THERE AREN'T MANY HARDCORE ANARCHIST CYPHERPUNKS LEFT IN THE ENVIRONMENT?

No, and certainly not in public forums where those who speak are people working professionally with these things. For good reasons, criminal types do not make themselves known here.

The tone of professional hackers today is far better than before, and the discussions are mostly technical.

HOW DID YOU GET YOURSELF INTERESTED IN THE WORLD OF HACKING?

My father worked in the IT industry and passed on a solid foundation and understanding of the subject at an early age.

It was my early passion for computer games and his efforts to get me to go to bed on time that evolved into an ongoing battle for control over our internet and initially spiked my interest in security.

Over the years, I kept coming back to security and expanding my knowledge base until it stuck with me as my primary profession.

At the same time, my father introduced me to coding and taught me about IT architecture. I wrote my first line of code as a teenager and developed a strong passion for security in the following years, that passion has only grown stronger since then. After high school, I started at DTU (The Technical University of Denmark) in Copenhagen, but a private company headhunted me before I got a chance to finish my studies.

HAVE YOU EVER PRACTISED ANY GREY ZONE HACKING YOURSELF?

No, I haven't. My interest in security related topics is from an intellectual point of view only, like solving a puzzle.

I study the same techniques as a malicious hacker in order to be able to get as close to the real scenario as possible, but the difference in the hat system is permission.

And I am very cautious about always having permission to break through the systems I test.

CAN YOU TELL US A LITTLE ABOUT YOUR TEAM?

I've built the team from scratch over the past four years. It's a team of real hackers and not just security consultants.

Our customers pay us to attack them, and we do so with all our skills. We find the back roads in the security systems, we close the gaps, and we look at the customers' general security infrastructure and help them raise the level of security.

DO CUSTOMERS COME TO YOU BECAUSE THEY HAVE SECURITY CONCERNS? OR DO THEY JUST WANT YOU TO CONFIRM THAT THEY HAVE THEIR SECURITY MEASURES IN PLACE?

It's mostly the latter. But if they claim to be in control of security, I offer them the first test for free. Because during my team's four years of existence, we have had a 100% success rate. There hasn't been an infrastructure yet that we couldn't compromise.

ARE SECURITY LEVELS IN GENERAL TOO LOW?

The standard today is typically set by the large accountancy firms, and this is reflected in the quality. The tests that are being carried out deviate more and more from technical penetration tests. They rely on questionnaires and checklists, which will only give a theoretical point of view. Emulating a real attack is essential if you want a realistic picture of the level of security. Testing today often doesn't reflect the way the hackers work. For example, a hacker will never use a scanner that is easily detected by the firewall. Skilled hackers use much more sophisticated types of attacks, and by only testing trivial things, companies are left with a false sense of security.

IF THE SECURITY LEVEL AMONG COMPANIES IS RELATIVELY LOW, HOW COME WE DO NOT HEAR MORE ABOUT HACKER ATTACKS?

I have wondered about that too, and my theory is that a lot of attacks are simply never detected by the companies. In addition, some companies would never admit if they were attacked.

HOW DO YOU EXPECT THIS TO DEVELOP IN THE COMING YEARS?

It's going to be a long and tough fight for companies to protect themselves going forward. Today, security is mostly a budget exercise placed on top of either IT or Operations. We are slowly moving towards it being taken on its own merits and we do see that it gets more attention, but we are far from where it is supposed to be. Over the coming years we will see more companies punished for being too slow in the transition, but also a larger group able to defend themselves.

But I hope that in the future, security will be something that must be part of any IT infrastructure. Security simply has to be built into applications and systems from the start.

SO WE NEED A FUNDAMENTAL CHANGE, A DIFFERENT ARCHITECTURE?

Yes, completely, because the technology used by most companies today was invented 20-25 years ago in a different era. Security companies just help their customers build on old security structures. But if you never start over, you will always have an old soft toffee lying underneath. And no matter how much you try to reinforce the security at the top, it's still unsustainable. You need to build security into the systems from the start; you need to wipe the slate clean.

TRENDS IN GLOBAL PAYMENT FRAUD

INTERVIEW WITH **ANDREJ EICHLER**, CMO FINANCIAL SERVICES AT WORLDLINE

Payment fraud is a major challenge for banks and merchants. But striking the right balance between preventing fraud and not causing any inconvenience for the customers can be very tricky. In this article, Andrej Eichler of Worldline identifies the most important current trends in fraud that banks and merchants should be aware of and also provides an overview of fraud in different geographies. Expert understanding of these two aspects of the fight against fraud is an essential element in Worldline's fraud risk management solution.

Over the years, fraud attacks have evolved and become more and more sophisticated. Thanks to Worldline's access to the vast amounts of data provided by banks and merchants, the company has an excellent overview of the preferred attack methods of criminals today.

> "Protecting banks and merchants requires a different approach but essentially the key part of their respective underlying missions is to provide stable, easy-to-use but above all else – secure services. Remove the security element and customers and consumers will take their business elsewhere – it's a proven fact. Reputational damage incurred due to poor fraud controls cannot be understated enough.

Andrej Eichler,
CMO Financial Services at Worldline

WHAT BANKS SHOULD BE AWARE OF

The vectors vary depending on the geography, but overall fraud targeting banks falls into the following four categories:

1. **Account Takeover (ATO)** - The main trend in fraud today is the account takeover. An account takeover happens when criminals gain access to a person's online e-commerce or financial accounts, often resulting in unapproved transactions and purchases.

   Due to COVID-19 and the global lockdown, there is currently an unprecedented number of ATO cases. One increasingly common trend is to send emails claiming to be from the World Health Organisation and promising information on protection against COVID-19[1].

   ATO attacks go far beyond traditional phishing (see below). The fraudsters know not only the card details but also the answers to all of the security questions (name of first pet etc.) and the account holder may not even realise that there has been a takeover.

2. **Traditional phishing** - Happens in all online channels. By phishing, the fraudster obtains banking or other payment information, e.g. when a seemingly genuine webpage/merchant asks the cardholder to reconfirm their log-in or payment data, but it is, in fact, a fraudster pretending to be the merchant.

   Phishing, like account takeover, has seen the single largest increase in the number of attempts since COVID-19 increased online activity all around the world.

   Predatory fraudsters have seen their chance and taken it, targeting consumers with increasingly believable scenarios in order to gain access to banking and other payment information.

3. **Malware** - Fraudsters are becoming more and more tech-savvy and malware is an ever-present threat.

   Malware can take the shape of keylogging, where the bank customer's computer gets breached by criminals who can steal any passwords that are entered, take screenshots, record viewed web pages, and grab any sensitive personal or financial information, e.g. credit card numbers, access codes and bank accounts.

   They are then able to send all the data to a remote computer or web server, where the person operating the logging program can retrieve it[2].

4. **Identity theft** - This is going one step further than ATO attacks and is a trend where Worldline is seeing rapid growth. The opening of bank accounts, loans and credits with falsified or illegally obtained consumer details has become very prevalent.

WHAT MERCHANTS SHOULD BE AWARE OF

When it comes to fraud targeting merchants, Worldline's experts have identified three leading trends, with a clear number one.

1. **Card not present** - The number one cause of fraud targeting e-commerce merchants is still stolen or breached card data.

2. **Account Takeover** - Compromised payment wallets or bank accounts are on the rise, which is caused by the increase in phishing attacks. It can result in serious reputational damage for the merchant, which can turn out to be very expensive to recover from.

3. **Friendly fraud** - Primarily seen with merchants and not banks, e.g. when a customer receives a package from a merchant but does not sign the receipt.

   This new type of fraud has also increased particularly because of COVID-19. Items ordered online are not being signed for due to the reduction in human contact. Worldline expects an increase in friendly fraud to hit later in 2020.

   According to the COVID-19 Commerce Insight dashboard, merchants have seen a 110% year-on-year increase in e-commerce orders in the US alone. Friendly fraud can account for between 40% to 80% of all fraud losses.

A GEOGRAPHICAL OVERVIEW OF FRAUD TRENDS

If a merchant is considering expanding their company and establishing branches overseas, they may want to consider learning about which types of fraud are trending on the continent they are targeting. This initial research may prevent foreseeable fraud attacks. Learning which threats local customers may be facing can also prove to be a valuable tactical investment. Ultimately, doing the initial research means creating the basis for great customer service.

North America - US commerce has been dominated by the use of magnetic stripe cards. When a lot of other countries switched to EMV cards, the US experienced an increase in fraud attacks. They acknowledged the advantages of the EMV cards and started migrating in 2014-2015. Currently there are around one billion EMV cards circulating within the US.

Europe - In Europe, stolen or compromised card details are still at the forefront of fraud. A high proportion of these cases are a result of the growth in e-commerce and the low use of strong customer authentication methods such as 3D-Secure.

Africa - In Africa, cases of phishing and social engineering, which is when criminals use social tactics instead of software hacking to gain access to a user's personal information, are still trending higher, reflecting greater access to technology within Africa, while these cases have decreased in Europe.

Asia - In Asia, there is still a lot of malware because some banks are not as well protected as they are in Europe for example. Compared to Europe, the single loss per fraud case is higher and the tendency Worldline sees is for fraud to be of a more technical nature, such as account takeover attacks.

Preventing all fraud, while at the same time not causing any inconvenience to customers, will probably still be an impossible dream for many years to come. No matter how much data an organisation possesses, it can also be hard to predict the future of payment fraud accurately, especially given the rise of new trends caused by unforeseen events such as the COVID-19 crisis. However, by continuously tracking the evolving technologies and trends in fraud around the world, Worldline is in an excellent position to help banks and merchants offer their customers a safer and more secure online experience.

1 https://www.cnet.com/news/as-coronavirus-crisis-worsens-hacking-is-increasing-security-experts-say/#ftag=COS-05-10aaa0j
2 https://www.malwarebytes.com/keylogger/

THE WORLD MAP OF FRAUD

Worldline has rolled out the big map and taken a look at fraud trends across the world as identified by some of the leading experts. The analysis and statistics displayed in this article are accompanied by commentary provided by Myles Simpson, Fraud Risk Manager in Business Development, Strategy and Innovation for fraud and risk products at EquensWorldline, Belgium, and Rodolfo Bertassello, Head of Fraud Operations at EquensWorldline, Switzerland, who has over 20 years of experience in issuing and acquiring.

FRAUD TRENDS ACCORDING TO EUROPOL

Card payment fraud qualifies as cybercrime, which is one of Europol's priority crime areas, called EMPACT under the 2018-2021 EU Policy Cycle. EMPACT targets the most pressing criminal threats facing the EU.

While card-not-present fraud is found across all sectors, in the EU there has been an increase in the use of compromised cards to purchase physical goods, airline tickets, car rentals and accommodation, according to the most recent data from 2019. You can read more about card-not-present fraud in the article on Global Payment Fraud Trends.

Worldline comments: "As more payments become digital, the transfer of funds becomes faster and new channels are developed, the risk of cyber-crime and account takeover remains high. Such initiatives from EMPACT, led by public authorities, provide for a better framework for collaboration between the public and private sector, which remains an important element in the international fight against crime.
Regarding the increase in purchases of physical goods, Worldline's research confirms that there is a rise in volume, i.e. how much money fraudsters spend per transaction, but notes that the amount of transactions has been flat since 2018 and will likely decrease slightly moving forward."

Counterfeit card-based fraud (counterfeit cards are often created by skimming, which duplicates the card's magnetic strip) is typically committed outside Europe. Due to the fact that the EMV payment method is not as predominant in other parts of the world as it is in Europe, card-present fraud has migrated, chiefly to the Americas and Southeast Asia, Indonesia and the Philippines in particular, where cards that have been copied in Europe are being used to retrieve cash at ATMs. The introduction of EMV technology in the United States has increased the focus on card-not-present fraud as EMV cards have reduced the number of card-present fraud cases.

WL comments: "CNP fraud is about 94% of gross fraud and counterfeit represents around 3%. We continue to see a steady drop in counterfeit cards as the migration to chip terminals and chip cards nears completion. The remaining counterfeit fraud is essentially done on ATMs outside Europe and usually in the same country as where the cards are being skimmed during the time the cardholder is travelling abroad.

Many issuers have started offering customisable payment cards for consumers that enable the consumer to block and unblock their card with their mobile phone in real time for e-commerce or to set daily spending limits. Another effective feature to avoid this kind of fraud is Geoblocking, where the customer can block individual countries or entire regions. Here the banks allow their customers to decide their own risk level."

The growing e-commerce industry is sparking further growth of card-not-present fraud, making it more lucrative for criminals as the prevention of card-present fraud becomes more effective. Newer payment options such as mobile contactless payment using NFC (near field communication) will not stop criminals from finding ways of abusing these new technologies. On the bright side, there has been a drastic decrease in cases of stolen PIN codes[1].

WL comments: "The decrease in cases of stolen PIN codes will likely mean a rise in social engineering (manipulating people into sharing personal information) in the future. As there is a drop in counterfeit fraud and magnetic stripe skimming, fraud due to account takeover or push notifications is increasing but certainly not to the scale as it was for counterfeit some years ago. Other elements need to be considered in the digital space, such as the fact that if a cardholder is manipulated to provide their credentials because of smishing or phishing or to transfer funds due to compromised business e-mail or malware, it can become difficult for the users to reclaim their losses, especially in the account transfer channels as money mules move money very fast and there is no direct 'chargeback' capability."

1 https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud

WHAT ABOUT BORDERLESS FRAUD?

Card-not-present (CNP) fraud has seen a significant increase throughout the EU. Multiple crimes are reported in many EU countries and the amount is increasing each year. One of the sectors most affected by CNP fraud is the airline industry.

WL comments: Of course, it always depends on how the data has been aggregated but in Europe the increase is mostly in digital goods (e.g.: mobile top-ups/something that can be resold) in the merchant category, which is predominant in terms of CNP fraud (up to 24% for Belgian cards issued by Belgian banks).

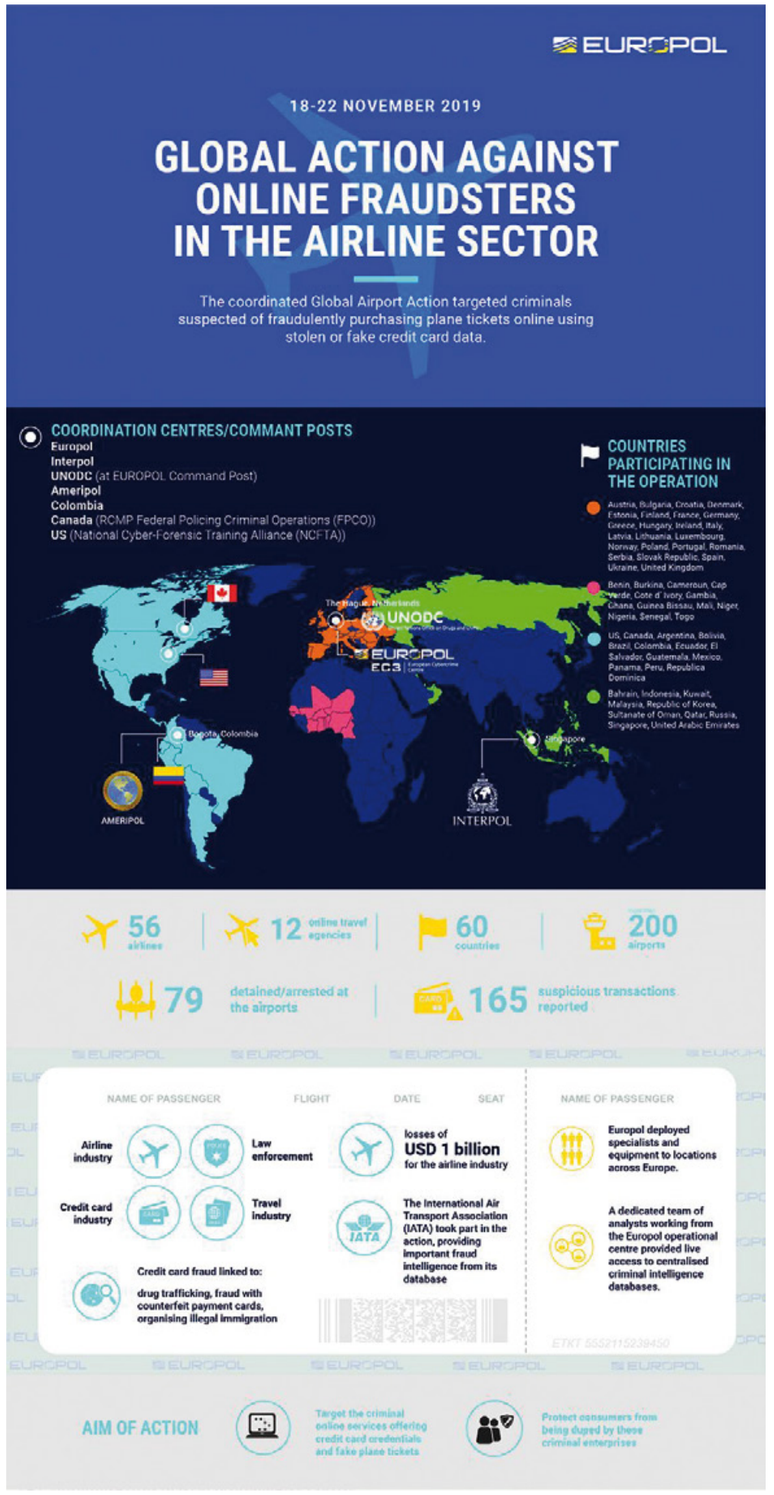
The airline industry's financial losses are estimated to have reached close to $1 billion per year, because of fraudulent online purchases of flight tickets. Fraud within this sector is very popular within organised crime and is often linked to more serious criminal activities including irregular immigration, human trafficking, drug smuggling and terrorism.

Global Airline Action Days (GAAD) is an international operation fighting fraudulent online purchases of flight tickets with compromised credit card data. The most recent operationtook place in November 2019 at more than 200 airports across the world, involving 60 countries, 56 airlines and 12 online travel agencies.

During the operation, 165 suspicious transactions were reported and 79 individuals suspected of travelling with airline tickets bought using stolen, copied or fake credit cards were arrested or detained.

"Airline ticket fraud is borderless by nature. This operation was the culmination of many months of meticulous planning between Europol, law enforcement, judiciary and border agencies, airlines and credit card companies, and is a perfect example of how our combined forces can make a distinctive contribution in the fight against these criminal syndicates operating across borders," said Wil van Gemert, Deputy Executive Director of Europol's Operations[2].

2 https://www.europol.europa.eu/newsroom/news/79-arrested-in-worldwide-crackdown-airline-fraud



3

3 https://www.europol.europa.eu/newsroom/news/79-arrested-in-worldwide-crackdown-airline-fraud

GEOGRAPHICAL BARRIERS ONLINE ACCORDING TO FORTER

Despite the worldwide web being indeed worldwide, some types of fraud are still limited by the physical realities of geography. While data theft may occur a continent away, surprisingly online shopping fraud is far less likely to cross continents. But fraudsters do frequently target other countries, particularly in regions such as Europe, where goods and services can easily cross borders[4].

STATISTICS ON THE LEVELS OF FRAUD IN DIFFERENT REGIONS AND CONTINENTS

Different regions on a broad spectrum, Europe, the Middle East, Africa (EMEA), Asia Pacific (APAC), Latin America (LATAM) and the Americas (AMER), are all affected by different fraud trends as well as different customer behaviours. The data generated from these regions can be organised into the following categories:

4 https://www.forter.com/blog/global-fraud-trends/

SEASONALITY

While EMEA's buyer population is virtually all located in the Northern Hemisphere and focused in Europe, APAC's and to some extent AMER's population is geographically spread more widely across the Equator, from North to South. Ultimately, this impacts buying patterns specifically within travel (air, land, and accommodation).

HOLIDAYS

While the holiday season in both AMER and EMEA (consisting mainly of Europe and Russia) peaks at the end of the year, including non-holiday dates such as Black Friday and Cyber Monday, holidays in APAC are spread across the calendar a bit longer, focused mainly between September until February. These holidays include Black Friday, Christmas, New Year, Local New Year, festivals and the most celebrated shopping spree in the world - Single's Day, originating from China.

DATA BREACHES

Data breaches are more or less borderless and have hit all around the world. In Europe there was the case of British Airways in 2018, in APAC Cathay Pacific and Aadhar were hacked in 2018 and in the United States there were the cases of Marriott and Saks in 2018 and 2020.

LOCALITY AND LANGUAGE

It makes sense to look at fraud with an emphasis on languages, because although English is the preferred language among fraudsters, other commonly spoken languages, e.g. Spanish or French, are popular as well. It is highly unlikely for someone who is not Chinese and does not speak Mandarin or Cantonese to use a Chinese card on a local website.

CROSS BORDER

Fraud across regional borders is more limited. AMER buyers focus on AMER websites, while EMEA buyers focus both on EMEA websites and to some extent AMER and APAC websites (mostly non-Europeans). APAC buyers focus on AMER and APAC websites.

REGIONAL VARIANCE

While AMER consists mostly of North America, English-speaking buyers and Spanish- or Portuguese-speaking LATAM buyers, EMEA consists of three continents and multiple languages. Another regional fact to take note of is that APAC is the most densely populated region, also consisting of many different languages.

WL comments: In Europe, debit cards are also used for authentication means and there are more and more tokens used for direct access. The risk has increased for account takeover and transfer of funds from account to account with stolen or phished credentials.

We expect that the use of debit cards will decrease in the following years because European consumers are discovering that debit cards have fewer chargebacks and will opt for a safer option like a prepaid card.

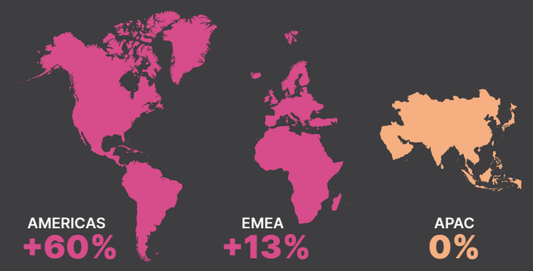
OVERVIEW OF INTERNATIONAL FRAUD TRENDS ACCORDING TO FORTER'S FRAUD ATTACK INDEX 2019

The market for fraud is incredibly dynamic and constantly changing in character and focus according to different regions. It is estimated that online merchants will lose $130 billion due to online payment fraud between 2018 and 2023.[5]

5 https://pages.ravelin.com/hubfs/All%20shareable%20content%20/Online%20payment%20fraud%20guide%20-%20website%20PDF%200619.pdf?utm_campaign=General&utm_medium=email&_hsmi=73321884&_hsenc=p2ANqtz--QYv2nnHZoCpdLS5J0iCRmCU9RfTaKbjFv8lH1aKT8RrKMwx-fVJpNMwLo5ZlofgFmyBUZ54vxDX64gDspG6aDkGV6Jg&utm_content=73321884&utm_source=hs_automation

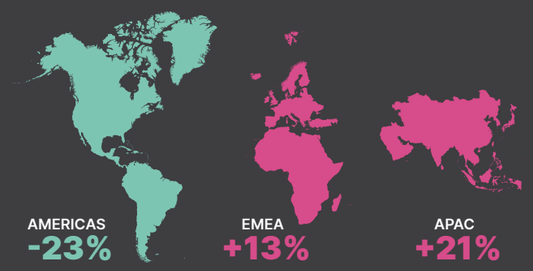
APPAREL AND ACCESSORIES (Fraud attack rates from Q2 2018-Q2 2019)

Fraud attack rates against the apparel industry have risen by 60% in the Americas. EMEA shows a lower increase, by 13%, while rates in APAC show no increase at all. Fashion items are perpetually in high demand and the products are easy to resell. Fraudsters buy the items and make a profit by reselling them for near retail price to bargain hunters.



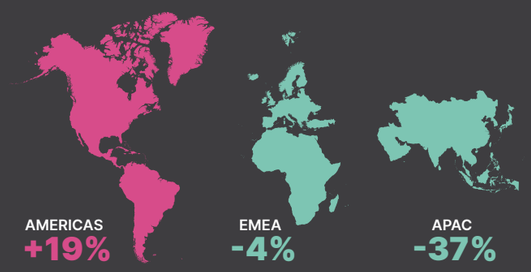
DIGITAL GOODS (Fraud attack rates from Q2 2018-Q2 2019)

EMEA and APAC show an increase, with rates of 13% and 21% respectively. This is mainly driven by an increase in demands for gift cards. For fraudsters, digital goods require minimum effort to cash out. In 2019, this industry saw a slight decrease in fraud attacks compared to 2018. This trend coincides with a wider trend that has appeared across e-commerce in general, which is a focus on quality of attacks versus quantity of attacks, meaning more targeted and detailed efforts providing better results.



ELECTRONIC GOODS (Fraud attack rates from Q2 2018-Q2 2019)

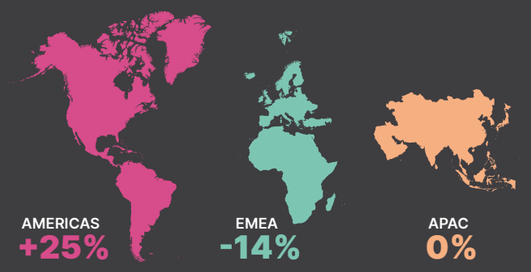
The increase in the Americas by 19%, is offset by the slight decrease in EMEA (4%) and the much steeper decrease in APAC (37%). Shoppers looking for a good deal on electronic goods often search to find the best bargain on third-party sites, where fraudsters can easily market their stolen goods for discounted prices.



JEWELRY (Fraud attack rates from Q2 2018-Q2 2019)

The jewellery industry has shown an increase in fraud attacks in the Americas (25%), offset by a 14% decrease in EMEA. This industry is very popular with online fraudsters because just one successful attack can mean an extremely lucrative payout.

6



6 https://cdn2.hubspot.net/hubfs/2776164/Fraud%20Attack%20Index%20Seventh%20Edition%202019/Forter-Fraud-Attack-Index-Seventh-Edition.pdf

Historically, merchants have viewed transactions originating from so-called high-risk countries such as Indonesia, Nigeria and Vietnam as no-go because these countries have fraud rates of up to five times higher than, e.g. the United States. But it is important to notice that the vast majority of the transactions emanating from these countries are actually legitimate. While merchants could have dismissed whole regions in the past, these areas are now transforming into growing markets. These countries have come to represent the fastest-growing digital retail markets and are overflowing with business opportunities.

But as the global payment and e-commerce systems shift, and the ways customers engage with brands and products evolve, online criminals are similarly adapting in the ways they interfere with and exploit online systems. The solution to this problem seems to be open communication. Cooperation and information exchange between the public or customers and the private sector is the most efficient way of fighting fraud, as in the case of the airline tickets, and all other forms of organised crime, such as irregular immigration, trafficking of humans and drugs etc.

WL comments: Public and private collaboration will remain an important driver of the fight against fraud. The priority must be on providing systems, services and law enforcement that are robust and stay focused.

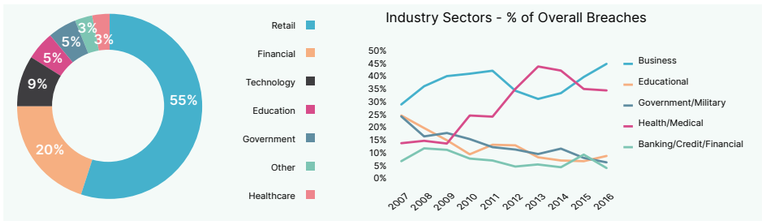
At the same time, we all need to ensure that those who are able to abuse the system pay for their misdoings and that those who are abused are not undermined.

BUILDING CYBER RESILIENCE THROUGH OPENNESS

Inspired partly by the airline industry, the payment and banking industry is now learning how to prevent critical events even better by judiciously sharing more information. Under the auspices of the European Central Bank (ECB), the Euro Cyber Resilience Board for pan-European financial infrastructures was established in 2018 with the overall goal of increasing the security level of the industry and preventing critical attacks from hackers and any kind of hostile organisation.

Whenever an airline experiences a critical incident, it must be reported to and analysed by an independent commission[1]. The idea is to continuously build up knowledge about potential risks and share it with all relevant parties in the industry - even though airlines are fierce competitors.

The goal is to prevent the same incidents from happening twice by practising openness, sharing information and learning how to do better in the future. This information sharing has been a standard procedure in this industry for decades, and it's likely to be one of the primary reasons for the astonishingly tiny number of fatal accidents in the airline industry today.



Data Records Stolen/Lost by Industry
Sources: WorldBank 2015 (left), Identity Theft Resource Center 201625 (right)

Unfortunately, a similar openness and knowledge sharing is not a practice you will find in a lot of other industries, for instance, not always in the payments and financial services industry. Payments have objectively proved to be one of the safest industries against cybercrime <ref>, at least in comparison to other industries. However, one can always do better. As cybercriminals get ever more sophisticated, network better and share experiences – so must the good guys. Especially in an industry, which historically has attracted hackers simply because the industry's core product is money, and which also attracts politically motivated hostile organisations because financial infrastructure is critical for modern societies.

TOWARDS STRONGER CYBER RESILIENCE - FRONTED BY THE ECB

Wiebe Ruttenberg,
Program Director Cyber Resilience Strategy of the European Central Bank

Therefore, things are changing in the payments and financial services industry. As part of an ECB cyber resilience strategy for financial market infrastructures (FMI), the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) came into existence in early 2018. **Wiebe Ruttenberg**, Program Director Cyber Resilience Strategy, ECB, says about the origin of the ECRB:

"The decision to establish the Board came during a meeting on cyber resilience with high-level representatives from pan-European FMIs, their critical service providers and public authorities, held by the ECB in June 2017."[2]

He recalls: "One participant in the June 2017 meeting formulated it pointedly: 'whether we are market participants or authorities, we all are victims of cybercrime and need to foster trust and collaboration among all of us in order to be able to address jointly the cyber challenges we all face.'"

In 2018, the ECB published the mandate for the ECRB, which describes that the objective of the new forum is to: "Enhance the cyber resilience of financial market infrastructures, which are active in the EU on a cross-border basis and clear and/or settle in euro (...), of their critical service providers and of the wider EU financial sector."[3]

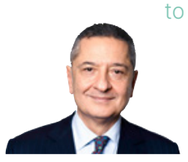
This objective should be achieved by: "Fostering trust and collaboration among pan-European financial market infrastructures and critical service providers, on the one side, and among them and authorities on the other side." And by: "Catalysing joint initiatives aiming at (i) increasing the cyber resilience capabilities and capacities of the financial sector including joint solutions and awareness, and ii) reinforcing the operational resilience of the financial sector generally."[4]

CYBER RESILIENCE WORTH BILLIONS

Mr Fabio Panetta, Member of the Executive Board of the European Central Bank, made a speech at the fourth meeting of the ECRB earlier this year where he underlined the importance of increased cyber resilience with some alarming figures showing the potential risk associated with a wide range of cyberattacks.

Mr Panetta said that cyber risk "is a danger which has the potential to trigger a systemic crisis" and that the total estimated costs of cyber incidents across all industries according to the report Systemic Cyber Risk by the European Systemic Risk Board has been estimated in the "range from $45 billion to $654 billion for the global economy."[5] Furthermore, he referred to Cybersecurity Ventures' Official Annual Cybercrime Report showing that "the average cost of cyber incidents had increased by 72% in the last five years and businesses will fall victim to a ransomware attack every 11 seconds by 2021."[6]

> "Cyber risk "is a danger which has the potential to trigger a systemic crisis" and that the total estimated costs of cyber incidents across all industries according to the report Systemic Cyber Risk by the European Systemic Risk Board has been estimated in the "range from USD 45 billion to USD 654 for the global economy.



Fabio Panetta,
Member of the Executive Board of the European Central Bank

CYBER INFORMATION AND INTELLIGENCE SHARING INITIATIVE (CIISI-EU)

When the ECRB was established in 2018, the ECB decided to evaluate the functioning of the forum after three years to see if it was making sufficient value and if anything needed to change. Since the three-year line has not been reached yet, it's too early to know what the result of the evaluation will say. However, based on Mr Panetta's speech, the ECRB seems to have got off to a good start, and the forum has already resulted in several additional initiatives including the Cyber Information and Intelligence Sharing Initiative (CIISI-EU).

The purpose of this initiative is to gather key players in the financial industry like payment service providers, central banks, stock exchanges, and clearing houses, and on an ongoing basis ensure that they share critical information and intelligence, and work closely together with Europol and ENISA (European Union Agency for Cybersecurity) to continuously and systematically strengthen the cyber defence of the finance and payment industry in Europe.

Wiebe Ruttenberg explains: "While the ECRB and - with it - CIISI-EU are 'closed' initiatives, aiming at a specific group of financial infrastructures and authorities, the philosophy and design of CIISI-EU can be a source of inspiration for other communities and stakeholders, within and outside the financial sector, within and outside Europe. Therefore, in line with the philosophy of the ECRB, we just published the CIISI-EU 'blueprint'[7] and anybody may use these documents in a flexible manner that suits their own specificities."

ON THE RIGHT TRACK

According to equensWorldline's Dr Michael Salmony, there is little doubt that the ECRB and associated initiatives like the CIISI-EU are tremendously valuable and have come to stay:

"With these new initiatives, we are definitely on the right track when it comes to fighting cybercrime and fending off and protecting ourselves from cyberattacks that, at worst, could create catastrophic consequences for our modern society."

1 In Denmark it's called Haverikommissionen. In France it's BEA, Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile

2 Quote from this page: https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html

3 https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ECRB_mandate.pdf

4 https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ECRB_mandate.pdf

5 https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html and https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

6 https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html and https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

7 See CIISI-EU - Cyber information and intelligence sharing: a practical example (ECRB Secretariat, Sept 2020) and https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html

KEEPING AHEAD OF THE FRAUDSTERS

Online fraud is one of the biggest threats facing merchants in 2020. Constantly evolving fraud attacks are making it hard for security systems to keep up. Worldline has developed a solution fully equipped for meeting and preventing old and new threats.

Worldline estimates online fraud in 2020 will total $25 billion, with 65% occurring in e-commerce operations. According to the European Payments Council's **2019 Payment Threats and Fraud Trends Report**[1], there is a long list of potential threats targeting an innovative market that is in constant evolution. While staying on top of e-commerce fraud and predicting attacks is no small challenge, Worldline's developers have made the prevention of e-commerce fraud a top priority, ensuring that the Worldline Fraud Risk Management solution lives up to their clients' expectations and needs.

UNDERSTANDING ONLINE PAYMENTS FRAUD

A major concern is that the criminals are changing their approach to card payment fraud and CNP (card not present) fraud. While fraudsters are focusing on more high-tech frauds like APTs (Advanced Persistent Threats), they are also reverting to older types of fraud, e.g. lost and stolen, sometimes in combination with social engineering. Among the various fraud cases related to e-commerce, CNP is still the most prevalent.

The primary factors behind fraud losses involving SEPA Credit Transfer and Direct Debit transactions continue to be impersonation and deception scams, as well as online attacks aimed at compromising data. The goal in these types of fraud is to obtain personal and financial details, which are then used to facilitate fraudulent transactions. In 2019 we saw an increase in Authorised Push Payment fraud.[2] This type of fraud is committed by criminals creating a very convincing looking invoice, including a logo and professional-looking format, and deceiving a business or individual into sending money to the criminals' accounts. The invoices can even come from an email address that the business or individual recognises, e.g. from a supplier. They may also call customers and get the information that way. The fraud is known as a push payment because a bank receives the payment instructions and authorisation to send money to another account.

MEETING THE THREATS WITH WORLDLINE FRAUD RISK MANAGEMENT

Efficient fraud prevention is not just a question of simply installing a piece of software. Fraud prevention starts with the merchant's knowledge of the customer's identity, shopping behaviour, shipping information and location data, in combination with biometrics (fingerprint, iris scan etc.), payment data etc. The trick is to combine that knowledge with the right fraud prevention tool, all without compromising the customer's experience. While merchants have to invest in the prevention of e-commerce fraud, the market demand for user-friendliness and simplicity is high, which can take the focus away from security resources. Finding the right balance between user-friendliness and security is a major challenge that merchants today need to address as a priority.

Rising to this challenge, Worldline has created a solution that helps merchants discover payment fraud while maintaining an optimal customer experience.

The solution controlled over 10 million transactions in 2016 and detected 99.4% of all the risky transactions that occurred. It has a response time of under a second, which is essential when monitoring fraud.

Worldline's Fraud Risk Management solution starts working even before the payment has taken place. The solution analyses the potential risks to the website before the customer has added any items to their cart. After adding the items, they are then analysed along with the information about the customer and the device used for ordering the items. The combined data allows Worldline to assess the risk of each order with a prescore. The payment page is then adapted according to the prescore result. As the shopper continues with the payment, the system analyses the payment data and the geo-location data. For each transaction, a final score is established to enable the merchant to accept or decline the transaction.

The Worldline Fraud Risk Management tool is not a one-size-fits-all solution but can be customised to the needs of every individual merchant, with Worldline's support team of fraud experts standing by at all times to meet the security demands.

KEY BENEFITS WHEN DEPLOYING THE WORLDLINE FRAUD RISK MANAGEMENT TOOL

Conversion rate increase: The fraud detection process will not stand in the way of the customer experience or risk the customer giving up on the purchase before check-out.

Reduction of false positives: More accurate fraud detection, preventing the merchant from potentially declining legitimate transactions.

Continuous anti-fraud tool improvement: Worldline provides the merchant with a tailored strategic recommendation based on an audit of their fraud records. This will optimise fraud prevention

Reduction of fraud costs: Proper fraud risk management will save the merchant direct revenue losses as well as indirect losses connected to anti-fraud management.[3]

1 https://www.europeanpaymentscouncil.eu/document-library/other/2019-payment-threats-and-fraud-trends-report
2 https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2019-12/EPC302-19%20v1.0%202019%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf
3 https://uk.worldline.com/en/home/solutions/merchant-services/security-fraud-risk-management/wl-fraud-risk-management-for-e-merchants.html

WL TRUSTED AUTHENTICATION

A STRONG RESPONSE TO FRAUD

As more and more payment services transition to online use, new risks and opportunities for fraud are emerging. In particular, the risk of fraud related to account takeover is increasing, as users have a limited ability to authenticate their identity in online situations. However, the WL Trusted Authentication solution provides a strong response to these issues and enables more secure online payment services. In this article, we evaluate the current environment for payment fraud and explain how WL Trusted Authentication can act as a reliable standard user tool for preventing payment fraud in the future.

PAYMENT FRAUD IN 2020

The behaviour of customers and fraudsters is constantly evolving through the development of technology. Additionally, both customers and fraudsters continuously adapt to each other. When fraudsters find new ways to intrude, customers incorporate new security practices into their daily operations. Likewise, when customers adopt new security solutions, fraudsters find other ways to commit fraud. This means that financial institutions have to constantly explore new ways to protect vulnerable parts of their payment processes.

While payment fraud in 2020 is perpetrated in several different ways, two general types of attacks can be highlighted. Firstly, there are attacks based on social engineering, which is a method in which the attacker manipulates their targets in order to carry out actions leading to fraud. An example of this is phishing, where the attacker uses techniques to acquire user passwords or credentials. Security in phishing attacks carried out over mobile devices is especially needed as an IBM study shows that "users are three times more likely to respond to a phishing attack on a mobile device than a desktop" (EPC302-19, 2019: p. 43). As well as securing the communication channels between financial institutions and users and maintaining user-friendliness, financial institutions also need to provide users with the ability to easily authenticate their identity.

Secondly, there are attacks carried out through WiFi interference, such as man-in-the-middle attacks where the attacker maliciously intercepts transmitted data between two parties by infiltrating the WiFi used. Using a cryptographic mechanism is therefore needed to secure the channel between the financial institution and the user.

INTRODUCING WL TRUSTED AUTHENTICATION

In the current payment environment, users require universal solutions that ensure the right balance between user-friendliness, simplicity and security, while meeting their daily needs for payment. Because of this, the financial industry is currently evolving rapidly and a high number of personal payment services are transitioning into online use. The rising tendency of accessing certain services online creates the need for strong authentication methods that can prevent intrusion from outside actors. Additionally, such methods must be universally deployed in order to ensure an end-to-end strong response to payment fraud. The WL Trusted Authentication solution is a key future component in fulfilling these requirements. WL Trusted Authentication is simple in its design, allowing all users to operate its features, while also complying with regulations such as PSD2, eIDAS and GDPR. WL Trusted Authentication is a potential game-changer in payment situations where establishing a secure user identity is critical. The solution enables secure authentication requests where the user needs to provide fingerprints, enter pin codes or use facial recognition, in order to maintain a secure channel for payments.

THREE KEY FEATURES OF WL TRUSTED AUTHENTICATION:

Simple delivery. When registration is easy, the solution can be easily deployed in massive amounts. The solution requires no hardware installation and operates directly from the internet.

Secure. All types of known attacks are prevented (phishing, man-in-the-middle, device theft, etc.). The solution is fully compliant with PSD2 RTS.

Easy-to-use. WL Trusted Authentication authenticates the user with a PIN code or biometrics (fingerprint, face-recognition, behavioural) and is suitable for remote use.

A MARRIAGE OF SECURITY AND ACCESSIBILITY

WL Trusted Authentication is a strong response to current trends in payment fraud. The solution protects against both major types of trending attacks (phishing and man-in-the-middle) while maintaining the user experience at a high level. The solution therefore allows for more secure payment situations without constraining the user – it simply adds a security layer while being compliant with PSD2 RTS and GDPR.

As described, the smooth registration process of WL Trusted Authentication allows for the solution to be deployed massively and universally. Consequently, the solution not only provides the right level of security for the current payment fraud environment but is also accessible for ordinary users connected to the internet. In the long-term, WL Trusted Authentication could become a the commonly used security tool for payments and almost any sensitive online operation. Like locks on doors or life vests in boats, the solution is a simple but standardised tool that can protect every type of user.

References:

- Wordline.com, 2020. *"WL Trusted Authentication"*. [Online]. Accessed 2. April 2020. Retrieved from: https://worldline.com/content/dam/equensworldline/documents/marketing-collaterals/WL-Trusted_Authentication.pdf
- CyberSource, 2019. *"2019 Global eCommerce Fraud Management Report"*. 2019 CyberSource Corporation. P. 1-23.
- EPC302-19, 2019. *"2019 Payment Threats and Fraud Trends"*. European Payments Council. Version 1.0. P. 1-91.

MAKING THE INTERNET OF THINGS SECURE

Thanks to the swift development of interconnected IoT devices, the business models of the future have the opportunity to become more autonomous. However, the focus during the development of the IoT has been more on the opportunities than on the security aspects and potential risks of implementation. In this interview, Minh Le and Thomas Blouin, IoT experts from Worldline, share their latest insights into the IoT & Security space and look ahead to future discussions and payment opportunities.

IoT (the Internet of Things) is a field in rapid growth. It is estimated that over 38 billion connected devices currently exist, which is triple the amount from 2015. At Worldline, IoT is seen above all as an enabler for reimagining business models: the company has already addressed several opportunities which enable autonomous transactions.

For example, insurance companies can set prices more dynamically based on data gathered from devices, while farmers can use IoT to monitor their land and livestock and share information. However, when incorporating devices and using data from IoT in these reimagined business models, it is critical to address the security aspect.

A QUESTION OF AWARENESS

Thomas Blouin explains: "There is a need today to create awareness regarding IoT and security. This is still a huge challenge. You need to create awareness from users, so that they accept the requirements related to security – this is not only technical, it is also about users accepting that there are some constraints."

The balance between IoT and security can currently be distinguished as a trade-off between the security aspect and convenience. Future IoT solutions will handle processes more automatically and conveniently for users, while making the security aspect more and more invisible.

The user needs to trust the devices to handle payments and services for them. Minh Le adds: "At Worldline we say that trust-invisibility is very important for IoT devices."

CURRENT RISKS

In the current IoT landscape, several challenges are connected to the relatively early stage of development of IoT. While the collection and use of data create several data-related risks around data theft or data privacy, the lifecycle of the devices can also create its own challenges, according to Thomas Blouin:

"Many devices are delivered with default settings which are not very secure (no password is set). There is no real compliance today for the mass market. When you buy a connected device like a smartwatch with payment capability, how would you manage a change of ownership, for instance if you want to resell the device?"

Minh Le points out that 80% of information collected from IoT devices today is processed by a central server in the cloud and only 20% is processed locally. He predicts that we will see a shift in the future from centralised to decentralised processing, where 80% of the information will be processed locally and 20% in the cloud. This creates an even higher risk of future data theft as intruders can access more data directly from the connected devices.

STANDARDISATION

For device manufacturers and the mass market, with today's focus on mass production rather than data-secure products, ensuring that the security aspect of IoT can keep up with the rapid deployment of devices will be a considerable challenge.

For Thomas Blouin, the future trend for IoT and security will require the implementation of standardisation and regulatory frameworks across the IoT space. "There are a lot of technologies and players. It has been kind of a 'wild west' for years. Some standards are emerging, some alliances are being formed as well, and we need to go that way and make the different players align. This is the major trend we expect, and it is already ongoing," he says.

Europe has taken a leading role in implementing initiatives for creating a safer IoT world, with the General Data Protection Regulation (GDPR) as one significant example.

PAYMENT OPPORTUNITIES

IoT creates interesting opportunities for future payment models in which processes become more automated and convenient for the user. Minh Le sees the emergence of four increasing levels of autonomous payments using IoT technologies:

- **Level 1 (Informational)** – The device can collect and send information about the user's bank account.
- **Level 2 (Permissioned)** – The device can trigger a low-level payment based on explicit consent from the user.
- **Level 3 (Conditional)** – The device can trigger a payment based on predefined conditions set by the user.
- **Level 4 (Full Autonomous)** – The device can trigger a payment without human intervention thus making it completely autonomous.

As the levels increase, the device gains more and more control of the payment activities, resulting finally in a fully autonomous payment model. Distancing the user from the payment process naturally makes the security level more invisible. Minh Le says that achieving this type of invisible security will be a major challenge:

"You need to educate the user about this increasingly invisible security and create awareness, making the user trust it and delegate the device to conduct payments. We have a long way to go. But we need to go through with it if we are to allow fully autonomous payments. And it will take years."

THE FUTURE OF PAYMENT AND IOT TRENDS

Minh Le says that the payment opportunities of IoT have been on the agenda at Worldline for a long time:

"We have a dedicated autonomous payment task force consisting of experts across the company looking at this topic. Consider for example the sharing economy and sustainability, where pay-per-use business models are emerging thanks to IoT as technology enabler. These are some of the things we need to tackle in the coming years."

It is still too early to define the shape that the future IoT payment model will take. However, Worldline has looked at three alternative payment models where IoT can impact how future autonomous payments will be made:

- **Card Scheme Payment Model** – This model is based on tokenisation mechanisms. Card tokenisation makes the IoT device able to conduct payments. Imagine a connected car hosting a tokenised card. The car would be able to pay for several car-related costs such as tolls, gas station services and parking.
- **Bank Credit Transfer Model** – This model is based on instant payments. Banks can execute real-time payments and let IoT devices trigger instant transactions between bank accounts.
- **Digital Currency Payment** – This model is based on blockchain technology and digital currencies. Due to the secure distributed ledger structure of blockchain, IoT devices can make digital currency transactions with or without a trusted third party.

Thomas Blouin expects the discussion around IoT use cases and security to continue to evolve in the coming years:

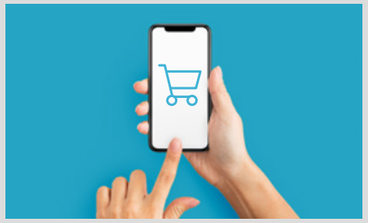
"We have changed from an IoT growth-focused world where the topic was 'what can IoT bring technically', to the question of 'how can the IoT data be used and what value does it have'. But also, how do we protect against an unexpected or unwanted use of the data? The 'how-to' in IoT is less in focus now. The question is then for what purpose we use the data."

It seems certain that we will be hearing much more about IoT in the future. If you want to know more about the potential of IoT for payments and other applications, do not hesitate to contact our expert Thomas Blouin at thomas.blouin@equensworldline.com.

THE WORLD AFTER COVID-19 DIGITAL EVENTS

Digitization is having a great impact – it can help organisations and socities within which they operate.

How we go to work, interact with colleagues and serve our customers has been and will continue to be transformed by digitization, now accelerated by COVID-19.



Digital Panel Series #1
ZERO TOUCH CUSTOMER EXPERIENCE

Digital Panel Series #2
ONLINE BY DEFAULT

Digital Panel Series #3
PURPOSE AND RESILIENCE

Digital Panel Series #4
DIGITAL ECOSYSTEMS

Watch these events and more on the **Worldline Bright Talk channel**

BrightTALK

STABLECOINS

STABLECOINS
NEXT GENERATION REGULATED DIGITAL CURRENCIES

Highly volatile cryptocurrencies with limited applicability have been around for more than ten years. But now that stablecoins are taking centre stage their practical use is back in focus. Both private companies and central banks around the world are using stablecoins for a wide variety of purposes.

More than ten years have passed by since Bitcoin first saw the light of day. Bitcoin was the implementation of a revolutionary, subversive idea aimed primarily at the incumbent banking system, and it came in a package of three elements: an underlying technology called blockchain; a decentralised peer-to-peer payment system; and a cryptocurrency called Bitcoin.

Fast forward to the present: The jury is still out when it comes to deciding on how innovative Bitcoin turned out to be. From one point of view, you could argue that it has been probably the biggest game-changer since the arrival of the internet, because of the potential of blockchain technology and the appearance of a completely new token economy. From another perspective, you could rightfully say that the financial system is more likely to gain advantages from the underlying technology rather than to be kicked out of the game – and that Bitcoin failed as a payment system.

WHY BITCOIN FAILED AS A PAYMENT SYSTEM

Let's focus on the last part and try to understand why Bitcoin for making payments didn't succeed, and how this led to the development of a new category of digital currencies which is now spreading around the world.

The question why Satoshi Nakamoto's peer-to-peer payment system is hardly being used anywhere today can be answered with one single word: volatility! A currency needs to be stable for people to start using it in their daily lives when buying goods, and Bitcoin is anything but stable. Despite not being backed by any asset or having any intrinsic value Bitcoin managed to become a popular – but extremely volatile – investment object. And to have such a thing as a currency is a contradiction in terms.

THE ARRIVAL OF THE STABLE CRYPTOCURRENCY

However, since a decentralised, peer-to-peer payment system based on blockchain technology is a really interesting idea, several individuals and companies around the world started to think about how to develop a cryptocurrency that would not become a victim of volatility; a cryptocurrency that would be as stable as a dollar or a euro. And out of this came stablecoins of which Tether, TrueUSD and DAI are some of the most well-known examples.

Common to all these stablecoins is that they are blockchain-based currencies backed by some kind of stabilising assets or collateral. It could be existing major fiat currencies like the dollar or euro – it could be precious metals like gold or silver or in principle any kind of collateral with a value. For some of these stablecoins, like DAI, the ideal situation is when the collaterals backing the coins are as diverse as possible (anything from precious metals, oil, real estate, or even intellectual assets of other cryptocurrencies) because a mix of asset types makes it less likely that they will all lose value at the same time.

FROM GOLD TO FIAT AND BACK

In 1971 Richard Nixon decided to abandon the gold standard for US dollars – known as the Bretton Woods System – and instead introduce what became known as fiat money. Fiat money has no intrinsic value; it is not backed by a tangible asset, but more vaguely by states and governments.

The stablecoin is in some ways a return of the situation before fiat (not surprisingly one of the stablecoins on the market is called TrueUSD). At the same time, it's an important step forward towards a more regulated, transparent and safe environment for cryptocurrencies. Replacing extreme volatility with stability opens up innumerable new use cases and makes stablecoins potentially more practical than traditional fiat currencies.

For these good reasons, stablecoins – just like the underlying blockchain technology – appeal not only to the crypto space but to a wide range of companies, organisations and regulators in the field of finance.

BUYING GOODS WITH GOLD

A current example is a stablecoin developed by Worldline on behalf of a Swiss client. The stablecoin which will go live early November 2020 is backed by 31.1 gram gold coins each with a value of approximately $1,250 minted by the Swiss company.

Worldline's Chief Innovation Officer, **Nicolas Kozakiewicz**, explains:

"The stablecoin is based on the gold coins that our client is minting. The coins all have a serial number: they are non-fungible. The client wanted to find a more convenient way of trading and exchanging those gold coins. Now, what we do is to put them in a bank safe and for each coin we create a certificate linked to a blockchain. Then we allow people with a digital wallet to acquire the certificates and make it possible for the owners to exchange certificates with other people from the same blockchain-based community. We use a private, permissioned blockchain so that the bearers of the certificates are known to the community through a thorough KYC (Know Your Customer) check."

"Furthermore, we use a trusted privileged access management (PAM) auditor to ensure that the certificates are not scams and that they are all linked back to the minted gold coins held in the bank safe. And the certificate allows the bearer to redeem the very gold coin that has the very same number as the certificate from the bank."

This tokenization process allows people to easily buy and trade the gold coins without ever having to move the actual physical gold coins around. They are kept safely in the bank, and only the digitized representations in the form of the certificates change hands.

However, while this certainly makes things smarter and smoother, it would be even better if certificates representing an ounce of gold with the value of around €1,250 could be divided into smaller bits that would, in fact, allow the bearer to use them as a currency when buying daily goods in the real world. And this is exactly what Worldline is enabling the Swiss client to offer their customers. Nicolas Kozakiewicz explains:

"The second step is the following: Since you don't spend €1,250 every day when buying food and goods, we have made a setup with a trusted third party that acquires the certificates and enables people to acquire fractions of these certificates. So now the certificate is divided into for instance 1000 fungible pieces of certificates all representing a small bit of an original certificate, which again is linked back to the gold coin in the bank safe. And these small gold tokens, which are stable because they are backed by real gold, will allow people to buy smaller goods with gold in ordinary shops."

Merchants that accept the tokenised gold coins part will receive these small pieces of coins, and the pieces can then be redeemed for genuine certificates that are directly linked to the original gold coins. This is what Worldline enables its Swiss client to do already, and Nicolas Kozakiewicz emphasises that a solution like this one could be adapted to any type of business.

CBDCS – NEXT-GENERATION STABLECOINS

The stablecoin solution described above is one of Worldline's most recent blockchain customer cases. However, Worldline has already been involved for more than six years in the development of asset-based infrastructure models that enable large-scale transaction throughput in safe environments based on private, permissioned blockchains.

The fact that these infrastructures are permissioned and private means that all participants will be securely authenticated and identified by the system. This makes it possible to create highly efficient consensus procedures that allow the systems to easily handle thousands of transactions per second – in contrast to the permissionless public Bitcoin blockchain which for security reasons has to be limited to a throughput of only seven transactions per second.

> "In Worldline, we are working closely with central banks and banks on this topic. There are two levels of CBDCs. The CBDCs used internally between central banks and banks directly, and the CBDCs used by you and me. They don't represent the same amounts of money, they don't have the same role and goal, and yet they are both currencies backed up by a state - and they are both called euro, pounds or dollars."

Nicolas Kozakiewicz,
Chief Innovation Officer at Worldline

Nicolas Kozakiewicz points out that blockchain is the likeliest vehicle for digital currencies in the future because it has been designed specially to help transfer assets in the digital world and because blockchains build on a mix of already known and tested technologies:

"It's really not rocket science; it uses three old and stable technologies: 1. hash systems; 2. digital signatures; 3. peer-to-peer networks. Put together, they enable us to build very interesting infrastructures, and we have lots of examples showing that it can be done relatively easily."

Within the space of stablecoins, Nicolas Kozakiewicz highlights Central Bank Digital Currencies (CBDCs) as a particularly interesting category. Central banks in several countries around the world are experimenting with issuing stable digital currencies for multiple purposes.

Common to both these types of CBDCs is that they can streamline a variety of activities and processes that are currently time-consuming and costly. A non-volatile guaranteed stablecoin that is used in secure blockchain infrastructure and even has a central bank issuer may help unleash the great potential of the token economy in the future. This may include optimising areas such as cross-border payments, clearing, settlement, reconciliation, etc.

"What we can really leverage with those technologies is a way to enable faster and more direct transactions in the financial industry. Take a very simple example: If I want to send euros from Paris to pounds in London today, it can involve up to 4-5 different banks, and both the sender and the receiver will have to pay accumulated fees. This antiquated system just doesn't make sense anymore, and now we have the technology to change it radically," says Nicolas Kozakiewicz, who continues:

"Lastly, the platform underneath stablecoins can be instantaneously used to trade other types of assets than digital-version-of-fiat-currencies. Whether a business needs to exchange for instance vouchers, property,

loyalty schemes or local currencies. The very same live platform will manage all these use cases."

IF YOU WANT TO KNOW MORE ABOUT THE DAVINCI TOKEN STABLECOIN, PLEASE VISIT **WWW.DAVINCI.GOLD**

THE DAVINCI GOLD TOKEN
RETHINKING GOLD INVESTMENTS

For many years, gold has been considered a steady and smart investment serving as a hedge against declining economic environments and rising inflation. According to the International Monetary Fund, gold is still of importance in today's society and economy even though it no longer backs any currencies like it used to 100 years ago. Investing in gold holds many benefits, e.g. during geopolitical and macroeconomic uncertainty, gold can provide financial cover and although the price of gold can be volatile in the short run, it has always maintained its long-term value[1].

While gold has acted as a currency since 560 BC and is well-established on exchanges worldwide, Swiss Gold Global Currency Corp SA (referred to as Gold Global in this article) has invented a new and innovative way of investing in gold through their DaVinci Token[2].

The DaVinci token is a new crypto gold concept consisting of stablecoins backed 100% by a 1 Troy ounce pure physical gold coin, which has been engraved using nanolaser technology on the hardened gold and registered securely on a blockchain. The gold is stored by BRINKS in Zurich, Switzerland.

The DaVinci Token is the title of a digital ownership of an irreversibly allocated DaVinci Gold Coin weighing one ounce of 24 carat gold. This innovative crypto gold concept was developed by Roger Kinsbourg, the founder of Gold Global, along with his co-founder team. The company was established in June 2016 and is now based in Geneva, where it is focused on the further development of the digital crypto gold concept.

The idea for the DaVinci Token was born in late 2015 to early 2016 when Roger Kinsbourg was reviewing his own investments. For a long time, he had been interested in both the historical and financial security that gold offers but was also intrigued by the opportunities of the cryptocurrency markets in general, Bitcoin in particular.

He realised that if he could invest in Bitcoin and hedge that with an investment in gold, then he would be able to mitigate some of the volatility in cryptocurrency investments. This was the beginning of the DaVinci Token. Kinsbourg carried out extensive research into cryptocurrencies, blockchains and the gold market and contacted people in his network with considerable experience in cryptocurrencies and blockchains. Their feedback assured Kinsbourg that this was an idea with huge potential.

In early 2016, Kinsbourg and two of his friends and associates established Gold Global Currency Corp S.A. in Switzerland. They chose Switzerland because of its historical reputation for economic and fiscal stability and the presence of major gold refineries smelting 70% of the world's gold production.

Gold Global's first goal was to mint and sell a 1 Troy ounce 24 carat pure gold coin of their own: the DaVinci Gold Coin. Meanwhile, they were also planning to create their own cryptocurrency backed by the DaVinci Gold Coin. Their vision was that their new Gold Global cryptocurrency would be represented by a digital coin/token, which would in effect be the title of ownership of their own gold coin.

GOLD GLOBAL'S VISION

Kinsbourg and his team knew that they had developed a concept that was unique compared with anything else on the market. The solution addresses a major problem for gold investors, who face constant logistical problems of secure storage, insurance, proving ownership and ensuring safe transportation once their gold is sold. Gold Global's vision is to store individual owners' new Gold Global gold coins in a secure Swiss vault, while also allowing them to pass on their ownership to others simply by transferring the title in the form of a digital token on a peer-to-peer basis via a secure private blockchain. This flow will bring liquidity to gold without the inherent logistical problems, while at the same time democratising gold investment by opening it up to almost anyone.

Roger Kinsbourg has set out to lead this new way of thinking about gold investments. His family has a multi-generational history with gold, going all the way back to his grandfather Julien Kinsbourg who was an early investor in the Alaska Klondike Gold Fields back in 1900. Since then, the Kinsbourgs have worked with gold as a safe and secure refuge of value in times of financial crisis, monetary uncertainty, economic and political turmoil and market volatility.

PURPOSE

The DaVinci Token is designed specifically to tokenize gold thereby enabling anyone to own and trade gold safely without the need for intermediaries.

Gold Global will officially launch the DaVinci Token in the coming weeks. At a later date, they will introduce two other tokens; the DaVinci Gold Crown, representing 0.001 gram of pure physical gold (please find more information below in the article) and a more substantial token, the DaVinci bullion, representing one kilo of pure physical gold. This further step will represent ownership of uniquely identified pure gold bullion, catering to the needs of Ultra High Net Worth investors wishing to hold physical gold in a safe and secure jurisdiction effectively under their direct control, without the intervention of any third party and at a significantly lower cost than they can find elsewhere.

For over four years the Gold Global team made many presentation, attended conferences and made roadshows building a wealth of contacts with individual investors, family offices, wealth managers, investment funds, private banks and trusts evidencing the true potential for this innovative way of acquiring gold to hold and/or transact worldwide.

PRIVATE BLOCKCHAIN

The Gold Global digital gold platform, backed by the company's own private blockchain developed in collaboration with Worldline and using the DaVinci Token as a stablecoin, provides clients with all the security they require.

Gold Global chose Worldline as their service provider to develop its blockchain because of Worldline's position at the forefront of the digital revolution. Worldline is the leading payment transactions service provider in Europe and the fourth largest in the world, handling billions of transactions on a daily basis. Gold Global also wanted to position itselfas a major, fully regulated stablecoin issuer in Switzerland in compliance with Swiss laws and the guidelines of the Financial Market Supervisory Authority, FINMA. The purpose was, to some degree, to distance the Gold Global team from the present cryptocurrency ecosystem and any potential controversy.

HOW IT WORKS

Interested individuals, companies and other entities can access the Gold Global onboarding platform via the company website at www.davinci.gold. As a first step, they must agree to the terms and conditions in order to use the website and then provide the usual personal information and other details internationally required for KYC (Know Your Customer) and AML (Anti Money Laundering) due diligence checks. If they do not pass these mandatory checks, then they will not be able to participate. Once they pass the checks, they will be permitted to buy DaVinci Tokens and the specific underlying gold immutably allocated to those tokens.

Once their funds have cleared for their purchase of DaVinci Tokens, Gold Global will set aside the specific DaVinci Coins or gold to which those tokens specifically relate, register them to the new owner in the Gold Global private blockchain and send the new owner a DaVinci digital wallet (in the form of a smart payment card). The newly registered client will then receive their digital DaVinci Tokens the moment they log into the DaVinci private blockchain.

Gold Global may later have the DaVinci Token listed on certain existing crypto exchange platforms with a specific app and/or launch a Gold Global exchange-bartering platform to enhance liquidity.

In a second phase, once the current DaVinci Token is fully operational, Gold Global will launch its second stable coin, the DaVinci Gold Crown, representing 100th of a gram of pure physical gold, which will be stored in secure vaults also with BRINKS in Switzerland and regularly audited by an independent custodian. At the current market price for gold, a DaVinci Crown would have a value of around €0.50-€0.60.

In essence, the DaVinci Gold Crown will become a new form of gold-backed cash. Owners of DaVinci Gold Crowns will hold them in their Digital Gold Wallet/smartcard or on a cryptographically protected smartphone app and be able to use them for payments at points of sale around the world via the Worldline international network. DaVinci Crown owners will also be able to use the DaVinci smartphone app to transfer their DaVinci Crowns to others as payment by using NFC (Near Field Communication) technology.

At any time, DaVinci Token owners will be able to request a redemption of their tokens for the allocated DaVinci Gold Coins by sending a simple notice to Gold Global. After the exchange has taken place, those specific DaVinci Tokens will be eliminated from the Gold Global private blockchain.

COLLABORATING WITH WORLDLINE

As mentioned earlier, Gold Global is collaborating with Worldline, a world leader in digital payment technology. Worldline is developing the private blockchain and all the other IT infrastructure and technology to ensure that the Gold Global platform runs smoothly from the very start of all its launch phases. Worldline will continue to work with Gold Global after the launch as the entire DaVinci Crown payment system will operate on the Worldline network backbone. Worldline will undertake the operation of the payments system as well as all the transactions and the creation of new digital DaVinci Tokens and Crowns.

Gold Global was looking for a partner with genuine blockchain industry-grade projects in the field, which it found in Worldline. Worldline has worked in close partnership with Gold Global in the design and development of its IT platform and private blockchain.

STABLECOINS AND DECENTRALISED FINANCE

There have been many implementations of stablecoins utilising blockchain technology, which is the objective of the DeFi (Decentralised Finance) movement. In Roger Kinsbourg's opinion, some of the stablecoins introduced so far are constructive and move the democratisation of money forward, while some others are more questionable and could even be considered as scams.

While he and his team are on a mission to advance the democratisation of money and gold, they have a very clear, value-added objective. They have made it a priority to comply with all the regulatory agreements of different countries and to be able to operate in full accordance with all laws and responsibilities, as any good company in the financial sector must do.

Gold Global's mission has become even clearer in recent years as national debt burdens have risen enormously in most countries around the world, with many large businesses and particularly financial institutions being propped up by government intervention. The printing of money by governments, through quantitative easing, has led to the effective devaluation of many currencies. On top of this, a global pandemic has virtually closed down the world economy.

The tokenization of gold in the form of stablecoins is the simple and modern way for people to enjoy the ownership and safety of gold, while also being able to use gold as a means for payment for goods and services. Furthermore, it paves the way to a decentralised alternate financial private monetary system, pegged to gold and self-regulated, which can provide certain regions with lesser-developed economies and inconvertible currencies with the solution they need for domestic and international payments and services for their underbanked people.

THE GOAL

The team at Gold Global are convinced that their model will be successful and will be an example to be followed by other stablecoins. Moreover, they are confident that their DaVinci Crowns will reconcile the two different worlds of the legal fiat currency and the decentralised cryptocurrency and show the way forward for other tokens and possibly for digital currencies issued by central banks.

Gold Global anticipates that the DaVinci Token and DaVinci Crown will create a new financial paradigm as stablecoins backed 100% by LBMA 999.9 pure physical gold. The end goal is for the Token and the Crown to form an important part of the foundations of a new, more democratic, decentralised financial ecosystem and a universal payment method.

1 https://www.investopedia.com/articles/basics/08/invest-in-gold.asp
2 http://davincitoken.com/

EDPIA
ADVISING EUROPE'S NEW PAYMENTS INDUSTRY

May 7th 2020 marked the launch of the EU advocacy alliance group EDPIA[1]. EDPIA stands for The European Digital Payments Alliance and represents European independent payment services providers. The alliance was established by French Ingenico Group, Danish Nets, Italian Nexi and French Worldline to contribute to the EU policy debates shaping the business environment for digital payments. Other mentionable goals are the strengthening of the visibility for policy makers and also to support the EU's vision of creating a Single Digital Market (SDM)[2]. On 3rd August 2020, they were joined by British SIA Group.

EDPIA wants to ensure a stable regulatory framework enabling fair and equal competition for all companies regardless of nationality and place of operation. Their work is based on the three pillars of SDM; Access, Environment and Economy & Society to guarantee easy access for consumers and businesses to European digital services and goods, equal opportunities for digital networks to thrive and compete and maximising the digital economy's growth potential.

EDPIA is a class example of competitors constructively joining forces to optimise the basic conditions for the market competition. EDPIA sets the standard for competitors working together to create the same conditions for everyone in the field, themselves included, on a more so lid foundation.

WHAT EDPIA STANDS FOR

The companies behind EDPIA have chosen working together to accelerate the completion of the Digital Single Market in order to enable frictionless digital payments.

Smooth and fast payments provide transformative potential for the Digital Single Market, which results in benefits for consumers, merchants, startups, SMEs as well as public institutions.

Digital payments play an important, societal role and is an important tool for promoting economic inclusion and therefore the key to preserving Europe's social market economy.

The payments industry is at the heart of the fourth industrial revolution, as it is an area with great potential for using new technologies. EDPIA also believe that they will strengthen the technological know-how in Europe.

The payment sector requires a versatile ecosystem, which is also recognized in The Revised Payment Services Directive 2 (PSD2) and the Interchange Fee Regulation. EDPIA will work towards strong European regulatory frameworks that enable fair competition.

EDPIA'S MISSION

Payments are an essential element connecting the people and the economy. But so far, payments have primarily been carried out in cash, cheques and electronic payment devices holding very limited and simple features. This has resulted in the success of the European Single Market but despite its successful development, the European Single Market has proven to be an insufficient framework. This leaves Europe with a massive need for a framework that allows everyone to carry out payments anywhere and anytime in a secure, digital, fast and cost-effective way.

These are the circumstances that have shaped EDPIA's mission, which is advising on how to build a diverse payments ecosystem in Europe. EDPIA will be doing so by creating a world-class European payments industry that reinforces the EU's competitiveness worldwide and supports Europe in becoming a global leader in payments innovation[3].

EDPIA also want to share their opinions on current news and events posing a potential impact on the payments industry, society and the political system in the EU. Recently, EDPIA have released their own analysis of the impact the COVID-19 crisis has had on independent EU payments services providers. Here they call on the EU policy makers to acknowledge the excessive increase in consumer claims for reimbursement and deferred solutions, which could lead to merchants losing the support of PSPs if the deterioration in credit risk continues.

They also found that EU PSPs have facilitated changes in consumer behavior to reduce infection risks via an increase in e-commerce and remote, contactless and mobile payments, while keeping the EU payments systems fully operational. EDPIA has also shared their views on the impact of EU Interchange Fee Regulation as well as an opinion piece on the European Payments Initiative etc.

EPI - EUROPEAN PAYMENTS INITIATIVE

On July 2nd 2020, 16 major Eurozone banks from Belgium, France, Germany, Spain and the Netherlands announced the launch of the European Payments Initiative (EPI). The EPI has been established to work towards the creation of a unified payment solution for consumers and merchants across Europe. The solution will be encompassing a payment card and a digital wallet and covering in-store, online and person-to-person payments as well as cash withdrawals.

EDPIA have taken an interest in EPI because they are working towards an increased collaboration between European stakeholders to provide payment services that meet the needs of European customers and strengthen the autonomy of the European retail payments market. It seeks to replace national schemes for card, online and mobile payments with a unified card and digital wallet that can be used across Europe, thereby doing away with the existing fragmentation.

EDPIA'S VIEW ON EPI

EDPIA welcome new payment scheme initiatives like the one from EPI and believe that EPI can prove successful, that they can get the necessary support from the payments industry and provide value for merchants and customers. Of course, this requires that they are based on a viable business model, including issuers, acquirers, processors and the scheme itself.

Gilles Grapinet, President of EDPIA, said 'EDPIA welcomes any initiatives that could foster the growth of digital payments, an open and competitive EU payments market, as well as initiatives that help strengthen Europe's position within the global payment ecosystem'.

The companies involved in EDPIA are highly aware of the need to strike an appropriate balance between all of them and that all applicable competition rules must be respected. It also implies that all relevant players in the payments ecosystem, including non-bank players, should be involved in the design of the scheme. It also requires the governance of a new payments scheme should involve all relevant parties across the retail payments value chain.

A balanced scheme would also incentivise rapid take-up and merchant acceptance. EDPIA therefore welcomes that European third-party payment services providers are individually being given the opportunity to decide if they want to become founding members of the initiative before the end of this year.

As an advocacy body focusing on EU policy, EDPIA's hope for the future is to enter a constructive policy dialogue with EU policy makers and other EU advocacy bodies to share general views on how to build a successful pan-European scheme.

1 https://ibsintelligence.com/ibs-journal/ibs-news/european-digital-payments-providers-launch-edpia-to-boost-frictionless-payments-in-the-eu/
2 https://www.edpia.eu/#aboutus
3 https://www.edpia.eu/our-manifesto/

IMPROVING THE CUSTOMER'S BANKING EXPERIENCE

Interested in hearing more about how to improve the customer's banking experience with the right channel mix?
LISTEN TO WORLDLINE'S WEBINAR ON THE TOPIC.

The world of banking is unrecognisable from a decade ago and this market disruption and transformation is likely to accelerate. The traditional role of the bank is disappearing, as customer lifestyles, new technologies and new forms of competition continue to influence the sector. Currently, there is still work to do to improve digital experiences and reduce the gap between the rapid evolution of consumer habits and the slower evolution of banking. After all, a smooth and satisfying customer experience is the key to success in winning customers' hearts.

Each customer journey is composed of a unique set of touchpoints across channels that must be designed to optimise customer convenience and satisfaction at any time. Improving the customer experience starts with understanding the use of the channels and specifying them. But what is the best way to build a compelling value proposition for your digital customers?

DIGITAL CONSUMER EXPECTATIONS

Digitalisation is a key factor – as it is for most industries. Investment in new technology is valuable and must be treated as an enabler, rather than as a pure cost or a forced purchase. There is a large opportunity for financial companies to both enhance the customer experience and create cost-efficiencies with the right use of digital channels and processes. The knock-on effect from more digitally enabled markets is that consumers' expectations and preferred interaction methods in banking are far more demanding than ever before. They expect to be able to transact and communicate with their service providers anytime, anywhere, using any device. Being continuously connected is becoming more and more important. Consumers have become used to seamless, highly personalised journeys across digital goods, retail and social media experiences, demanding an always available service with a choice of channels.

CONSUMERS KEEPING CONTROL

Consumer behaviour in banking has already changed significantly, with customer interaction patterns sending a clear message to banks that consumers expect the financial services industry to follow suit. An increasing number of banks, for example, are already offering their services on mobile channels, allowing prospects to open new accounts and customers to subscribe to additional products 100% online. However, it is important to keep in mind that customers do not care about the channels themselves. Consumers want to keep the choice between digital and human interactions; they want to keep control. They care about experiences, about solutions, about ease and simplicity. Besides that, they favour a mix of interactions. Understanding why a customer would prefer one channel over another is essential. Use the latest devices but always focus on convenience for the consumer.

MARKET DISRUPTION AND DISINTERMEDIATION

With consumer preferences shifting, financial players must now compete on customer experience. This challenge has become greater still with the wave of new market entrants and the rise of Fintechs and Bigtechs in the financial services ecosystem. The agility and speed to market of these new offerings mean they are bound to capture consumers' attention and present a threat to traditional banking players who have not sufficiently invested in their customer experience capabilities. This means that banks, as well as other financial players, will need to push their boundaries and business models to rethink the way they approach their transformation roadmap. Big names from other sectors are busy building a digital-first, customer-centric offering from the ground up, often alongside more traditional players in the banking space. For example, Google is now offering payment accounts (with Citibank), Amazon is hyper-focused on developing financial products (with J.P. Morgan), and Apple has successfully launched its Apple Card (with Goldman Sachs). Competitors evolve quickly; it is important to evolve along with them.

THE ERA OF OPEN BANKING AND PLATFORM MODELS

Both within and outside the payments industry, platform models are gaining traction, and new integrated ecosystems are blossoming. While creating compliance and technical challenges, PSD2 has also helped to sketch out the first contours of the incoming 'Open API' era in banking. It offers a way to unleash the value of banking and payments data, opening up a new type of economic model for banks who want to build out new services by leveraging open API connections and partnering with other providers to bring innovations to their customers and better serve end-to-end customer journeys. Soon, end-customers will benefit from a wide array of integrated services to cover their long-term, personalised journeys, completely agnostic from individual providers or even the banking industry. Bank incumbents might still perceive multi-brand ecosystems as a major threat – but they may greatly serve to support a more customer-centric strategy. This Banking as a Platform (BaaP) approach will undoubtedly provide a strong route for banks to circumvent some of the constraints of legacy platforms and build stronger customer relationships.

MANAGING CHANGE

Ultimately, the fast pace of digital adoption among consumers has set unreasonably high standards for most financial institutions who are often hampered by their ageing legacy systems, inadequate IT resources and constrained budgets. These issues can make it difficult for incumbent banking providers to drastically rethink their digital strategies as they look for ways to compete. Financial institutions must now cope with new (digital) banking habits and find ways to adapt and respond more quickly to market changes. What banks may need to do is look at the changes they have to make due to compliance necessities and find ways to leverage the assets that these changes can create. This may provide access to new opportunities and innovations.

Mathieu Barthelemy,
Global Product Manager
Digital Banking,
equensWorldline

E-PAYMENTS CHALLENGE
CO-CREATE A DATA-DRIVEN LESS CASH SOCIETY IN EXTRAORDINARY TIMES!

During the COVID-19 pandemic, individuals, companies and society in general have been affected in ways one could not have predicted at the start of the year. Various industries have had to rebuild their business models and accelerate the pace of digital transformation at this exceptional time.

At the same time, the pandemic has accelerated the emergence of the cashless society and the arrival of the open data economy. It is changing the way we shop, the way we pay, how we manage our money and the way we authenticate our identities online. Supporting digital tools and services have become the focus of this transformation.

At Worldline, Europe's largest payments and transactions player, we believe that co-creation holds the key to transforming the world of payments. Thus, we established a unique business platform – the e-Payments Challenge.

In September 2020, Worldline organised the third edition of the e-Payments Challenge. The event was dedicated to payments, innovation and co-creating the e-payments ecosystem. The challenge convened a global community of Worldline customers, partners, fintechs, startups and industry thought leaders, all coming together to explore the digital transformation of the sector and help accelerate innovation-to-business.

This year, the fully digital event focused on three key themes: financial sustainability, consumer experience and digital disruption.

Financial sustainability is critical to the future of our society, now more than ever. We believe that innovations for personal finance and business finance will help people and companies put their finances on a more secure and efficient footing. We are also spearheading a new approach to cybercrime, based on sharing information and deploying biometric technologies.

The consumer experience will be at the heart of this new economy in which an omni-channel approach will be the status quo. Innovations such as distance payment, voice commerce and autonomous retail will play a critical role in shaping a seamless, safe and efficient customer journey.

Going forward, digital disruption will transform contemporary life. E-payments technologies are the starting point for this change. The potential for fundamental changes to the world of payments, currencies and data processing is enormous. Machine learning will help traffic drive freely in city streets. Blockchain will reshape supply chains and improve consumer confidence. Governments and banks will be able to introduce new digital identity services which will transform society.

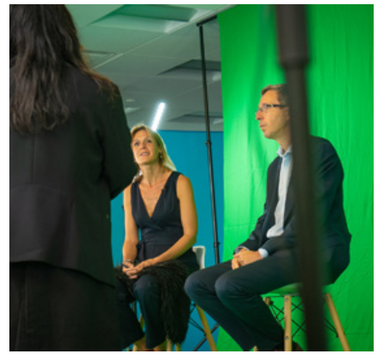
Payments and transactions serve as the circulatory system of the global economy. At Worldline, we believe that the possibilities for meaningful change are limitless.

We collaborate with like-minded partners to shape the future through co-innovation which lies at the heart of our strategy to continue to thrive in this extraordinary time.

DOWNLOAD OUR LATEST INNOVATION PLAYBOOK TO DIVE INTO THESE THREE TRENDS

THE MAKING OF THE DIGITAL E-PAYMENTS CHALLENGE

Behind the scene: Worldline yearly co-creation event has gone digital!



As you can see in the picture, our green-screen studio is located at Worldline's headquarters in the Paris region. Thanks to our team, we had two different green screens and four display screens to support this incredible online event. Have a look at our amazing backstage!

Thanks to this green-screen technology, we succeeded in providing a live opening keynote, which shed light on the e-payments sector within the context of the COVID-19 pandemic and discussed how co-innovation holds the key to continued growth. We also presented to our participants our production of Jack's journey, a completely immersive experience which explores the next generation of e-payments innovations and showcases solutions for tomorrow's e-payments' ecosystem.

If you want to know more about our innovative customer journeys, please browse our interactive user stories map and explore Worldline's solutions linked to use cases. And don't miss this chance to discover and share some of the best moments from our 2020 e-Payments Challenge, our photos and sketches gallery.

Finally, we would like to invite you to participate in Worldline's future innovation workshop and help us co-create the future of the payments industry. For more details about the innovation workshop, please contact Anne-Céline Muller and Michäel Petiot.

ABOUT WORLDLINE

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry and #4 player worldwide. With its global reach and its commitment to innovation, Worldline is the technology partner of choice for merchants, banks and third-party acquirers as well as public transport operators, government agencies and industrial companies in all sectors. Powered by over 20,000 employees in more than 50 countries, Worldline provides its clients with sustainable, trusted and secure solutions across the payment value chain, fostering their business growth wherever they are. Services offered by Worldline in the areas of Merchant Services; Terminals, Solutions & Services; Financial Services and Mobility & e-Transactional Services include domestic and cross-border commercial acquiring, both in-store and online, highly-secure payment transaction processing, a broad portfolio of payment terminals as well as e-ticketing and digital services in the industrial environment. In 2019 Worldline generated a proforma revenue of 5.3 billion euros.

worldline.com

For further information
infoWL@worldline.com