

Financial IT

Innovations in FinTech

DIGITAL CONSUMERS: BORN OR MADE?

Stefan Merz

Chief Operating Officer,
PPRO Group

CHALLENGER AND NEOBANKS

Mary Connor

Director, Product Management,
Retail Banking,
Finastra

DATAVISOR – EMBRACING PROACTIVE APPROACH TO FRAUD MANAGEMENT

Yinglian Xie

CEO and Co-Founder,
DataVisor

Nicolas Muhadri

Chief Executive Officer,
StreamMind

THE RISE IN BANK TRANSFER FRAUD: CAN YOU AFFORD TO LOSE OUT?



OPEX SUMMER

BUSINESS TRANSFORMATION
LEADERS SUMMIT 2019



26-29 August 2019 |
San Diego, CA Hilton San Diego Resort & Spa

DELIVERING OPERATIONAL TRANSFORMATION THROUGH PROCESS IMPROVEMENT AND DIGITAL EXCELLANCE

CORE THEMES

- Leadership
- Engage and Empower
- Technology Adoption and Enhancing Digital Capability
- Design Thinking
- Customer Centric OPEX Strategy

**USE CODE FIT_10 TO GET
10% OFF YOUR PASS!**

Check out the
Agenda
online!

Chief Data Analytics Officers, Fall

- Revolutionize Your Data & Analytics Strategy •
 - Drive Internal Transformation • Boost ROI •
- cdao-fall.coriniumintelligence.com

November 18–20, Boston MA



Corinium
connected thinking

Join the Largest Gathering of
Data & Analytics Executives
on the East Coast!
Save \$100 on your Pass with
Promo Code: FIT100
#CDAOFall

THE VIEW FROM AMSTERDAM

417 Years after the invention of the multi-national corporation, what are the themes that matter?

Money 20/20 Europe takes place this year in Amsterdam on 3-5 June. Given the city's contributions to global economic and financial history over the centuries – including the formation of the world's first modern multi-national corporation, the Dutch East India Company, in 1602 – it is appropriate that this edition of Financial IT is devoted mainly to the conduct and funding of cross-border trade. As one of our contributors points out, some 56% of consumers shop beyond their geographical boundaries in 2019.

As was the case in the early 17th century, a lot of trade and economic activity that is taking place is completely unregulated by governments. What our Publisher Chris Principe describes as System D – the Gray Economy – is growing steadily. This is mainly due to innovative technology – including virtually zero cost telecommunications and new payments systems. The opportunities are huge, even if the main beneficiaries are not necessarily going to be established financial institutions. As Chris notes, the unbanked do not need banks.

The complete lack of government involvement in trade, commerce and finance is not necessarily a good thing. Many of the contributors discuss the prevalence of financial crime – which is one of the central themes in this edition of Financial IT. Financial crime involves money laundering, which appears to be more of a problem for some institutions than others. As one of our contributors observes, the fines for money laundering that have been levied by US regulators on European-based banks are over five times as large as the fines imposed on US-based banks.

Financial crime also involves fraud against consumers and customers – a problem that is evolving following the introduction of the European Union's second Payments Directive (PSD2). Fortunately, as several of our contributors explain, technology is providing new solutions.

While consumers and customers face increased risks of being victims of fraud, the (much) bigger trend is that they are being empowered by the new technology that is being deployed by FinTechs and established institutions. This is another central theme of this edition of Financial IT. As one of our contributors points out, about one eighth of global retail sales takes place through e-commerce transactions, in a world where a significant – and growing – number of consumers have no recollection of a world without the Internet. Fees of payments services providers are moving downwards, while the needs for improved user experience are moving upwards.

Crucially, the empowerment of consumers and customers by technology involves new concepts of where retailing of goods and services actually takes place. The lines between social media platforms and market-places have become very blurred. Open Banking means that challenger banks, digital banks, neobanks – or whatever one wants to call them – have tremendous scope to deliver financial products that are manufactured elsewhere. Open Architecture – a well-established concept in the world of mutual funds – should flourish in the new world.

Just as new financial solutions and ideas came from the Netherlands in the early 17th century, new financial solutions and ideas are coming from other parts of Europe in the early 21st century. This edition of Financial IT includes varied contributions from experts in Hungary, Romania and Scandinavia. Europeans continue to play a central role in the (r) evolution in global trade and commerce. We wish all participants in Money 20/20 Europe a successful conference.

by Andrew Hutchings, Editor-In-Chief, Financial IT

Financial IT

Innovations in FinTech

Although Financial IT has made every effort to ensure the accuracy of this publication, neither it nor any contributor can accept any legal responsibility whatsoever for consequences that may arise from errors or omissions or any opinions or advice given. This publication is not a substitute for professional advice on a specific transaction.

No part of this publication may be reproduced, in whole or in part, without written permission from the publisher. Entire contents copyrighted. Financial IT is a Finnet Limited publication. ISSN 2050-9855

Finnet Limited
137 Blackstock Road, London, N4 2JW,
United Kingdom
+44 (0) 208 819 32 53

Founder
Muzaffar Karabaev

Editor-In-Chief
Andrew Hutchings
andrew.hutchings@financialit.net

Publisher
Chris Principe
chris.principe@financialit.net

Project Coordinator, Managing Editor
Katherine Emirosan
kemirosan@financialit.net

Content Editor/Events
Nilyufar Sodikova
nilyufar.sodikova@financialit.net


Multimedia Editor
Bekhruz Khazratov
bekhruz.khazratov@financialit.net

Production/Design
Timur Urmanov

Follow Us

 **Twitter** [@financialit_net](https://twitter.com/financialit_net)

 **LinkedIn** https://www.linkedin.com/company/rfp-connect_2

 **Facebook** <https://www.facebook.com/financialit.net/>

COMARCH

global presence
55 subsidiaries
90 offices in **31** countries
over **6000** employees
over **25 years** of experience

COMARCH FINANCIAL SERVICES

Comprehensive suite
of IT solutions for the
financial industry



Corporate
Banking



Private
Banking



Digital
Insurance



Cyber
Security



Anti-Money
Laundering

SYSTEM D: THE GRAY ECONOMY

System D is the underground or gray economy where approximately 20% of the world's population works and is about 20% of the world's total economic activity.

The term System D is adapted from the French word débrouillard. A débrouillard is a resourceful and self-reliant person that can figure out how to get what they need regardless of the obstacles. It was born from the mistrust of outsiders "étrangers"



Pepe Le Pew, a cartoon character, is a French striped skunk, constantly in search of love and appreciation

in medieval France when there was a real fear of trusting others for help. It possibly explains the against-the-grain French way of doing things which at times is not understood by foreigners. Interestingly there are few Frenchmen débrouillard from the past 50 years as the former French Colonies of Africa and Asia produce the débrouillard's of today.

The obstacles in the gray economy are usually the laws, price controls or taxes put in place by the state.

A decade ago, The Organization for Economic Co-operation and Development (OECD), estimated that around 1.8 billion people had unofficial jobs generally unregulated, untaxed and unbanked. The gray economy provides for a lot of débrouillards in this world.

Much of System D (débrouillards) are by circumstance rather than choice. Some live in countries like Venezuela, Zimbabwe, Central African Republic or Nigeria where the only way to buy the goods and services they need is by breaking the law. Venezuela is a great example. Consumer basics like food and medicine are no longer available in stores or pharmacies. The only way to get them is through System D.

Most of us have participated in System D transactions, whether we were aware of it or not. If your neighbor fixes your car and you slip him something, you've participated in the gray market. Or if you pay your handy man, housemaid or landscaper with cash. And there's no

guarantee the seller you bought from in the outdoor market reported their income.

Governments hate gray markets because they can't control them.

Even though governments blame the gray market for their economic woes, ironically, débrouillards may be the reason their economies are doing well. Now, we also know that there is a dark side containing crimes including human trafficking, drugs, weapons, cybercrime, hackers, fraud, counterfeiting, etc. all have a part of the gray market economy. Many of these débrouillards are master criminals, ruthless scammers, heartless killers, drug pushers, etc.

This is where the gray market turns into black-market activities with its newest version the DarkWeb. This is the newest growth area for criminals. The DarkWeb is an area of the internet invisible to most search engines, except through specialized browsers where illegal transactions are carried out in cryptocurrencies like bitcoin.

Governments focus on black markets as there are identifiable victims, but they knowingly include the gray market here as they seek control of markets, taxes and information on everything you do. They want us to see gray and black as the same, we must not fall for that propaganda. System D activities involve voluntary transactions between

willing buyers and willing sellers who are basically off the governments grid.

This includes our financial industry which the government regulates and has made them the watchers and data repositories of all that we do with our earnings. The banks also see a great opportunity in closing out the gray markets. Today they miss out on deposits, loans, insurance, mortgages, investments, etc. because the gray markets operate without the friction of bankers. Bankers are full partners with governments to push the often-draconian measures that are forced on small business and individuals. All in the name of protecting us from criminals they have injected themselves completely into the privacy of our finances. These rules and regulations are made to keep all of us inline with the perfect cover of fighting crime for our protection.

The Unbanked do not need Banks!

I like the carefree sound and friendly reassurance of this phrase. At the same

time, it is an important truth: All the Unbanked needs is a way to pay and get paid that is easy and inexpensive. Banks and credit card providers cannot do this, and it would not be profitable for them if they did. They are not here to help the low-income people. They are here to expand their business into a new demographic. They see about 2 billion people that they are not collecting fees from and what a growth area that potentially is. The problem for these people is that if they make \$100 in a month and the credit card companies get there 2% to 3% and the cost of having a bank account is a few more percent, it sounds small. What it means is that these people will be working 2 to 3 days each month just to pay these seemingly small fees. This is criminal and no morally sound person should let this happen.

What happens in the gray market is not simply by chance. It has intelligence, resistance, organization, group cooperation following thought out but unwritten rules making this a system, System D.

System D offers the opportunity for many people to be productive and take care of their families. No job-cutting, factory moving or offshoring your job here. Rather, a street market boasts dozens of entrepreneurs selling similar products and scores of laborers doing essentially the same work. Even in the most difficult and degraded situations, System D merchants are seeking to better their lives.

While the governments together with the banks claim to be in favor of and to support free markets, they think things work better, with trade barriers, phony tax cuts, fake money, fake interest rates, regulations, controls, etc., but they can't. Governments are lending fake money at fake rates, the banks get their fees and big corporations earn fake profits and buy back their own shares with free money. People are starting to realize that government produced money is worthless and that value is in real historic holders such as gold, silver, land, etc. They want to believe that we don't see or are not smart enough to know, but the gray market continues to grow.

Finnovation
World | Kenya
18th June 2019, Radisson Blu, Nairobi

-- I am Speaking as a --
Keynote Speaker
at
Finnovation
World | Kenya
18th June 2019, Radisson Blu, Nairobi

Chris Principe
CEO | Solidus Global, Ltd
Publisher | FinFuture & Financial IT

FinTech and the Positive Transformation of Banking in Africa

Get Involved
Finnovationworld.com/
[@Finnovationlive](https://twitter.com/Finnovationlive)

Follow us on
ritu@finnovationworld.com
 Finnovation Fintech World Series

Use My Code To Avail Discount: PRINCIPE2019FK

EDITOR'S LETTER

- 2 THE VIEW FROM AMSTERDAM**
 417 years after the invention of the multi-national corporation, what are the themes that matter?
Andrew Hutchings, Editor-In-Chief, Financial IT

COVER STORY



- 18 THE RISE IN BANK TRANSFER FRAUD: CAN YOU AFFORD TO LOSE OUT?**
Nicolas Muhadri, Chief Executive Officer, StreamMind

INTERVIEW

- 24 COLLABORATION THE KEY TO FIGHTING FINANCIAL CRIME**
Gillian Shaw, Manager, RBR
- 32 HYBRID ADVISORY MODEL: MEETING THE NEEDS OF GENERATION X AND GENERATION Y SAVERS AND INVESTORS**
Imre Rokob, Director of Business Development, Dorsum

PUBLISHER'S LETTER

- 4 SYSTEM D: THE GRAY ECONOMY**
Chris Principe, Publisher, Financial IT

LEAD STORY

- 10 CHALLENGER AND NEOBANKS**
Mary Connor, Director, Product Management, Retail Banking, Finastra
- 26 DATAVISOR – EMBRACING PROACTIVE APPROACH TO FRAUD MANAGEMENT**
Yinglian Xie, CEO and Co-Founder, DataVisor
- 38 DIGITAL CONSUMERS: BORN OR MADE?**
Stefan Merz, Chief Operating Officer, PPRO Group

FEATURED STORY

- 8 HISTORY REPEATING ITSELF? THE GREAT BUNDLING DEBATE**
Pat Patel, Global Content Director at Money20/20 for USA, China, Europe and Singapore
- 14 SEIZING THE OPEN BANKING OPPORTUNITY**
Georg Ludviksson, CEO & Co-Founder, Meniga
- 16 TIER TWO BANKS: IS THERE A FAST-TRACK TO A CHALLENGER UX?**
Lars Sandtorv, Chief Executive Officer, MeaWallet
- 21 PSD2 APIs: ARE YOU READY TO RESPOND TO THE NEW FRAUD THREATS?**
Robert Tharle, Fraud and Authentication Subject Matter Expert, Nice Actimize

30 FINANCIAL OPERATIONS MADE EASY

Ioana Guiman, Business Development & Managing Partner, Allevo

34 INCLUSIVE BUSINESS BANKING IS NOT CLOSE ENOUGH FOR SMES

Anders la Cour, Co-Founder and CEO, Banking Circle

36 WHAT ARE THE KEY TRENDS DRIVING PAYMENTS ACROSS EUROPE?

Gertjan Dewaele, Head of Innovations, Ingenico ePayments

42 LOOK NORTH TO NAVIGATE eID SUCCESS

Arne Vidar Haug, Chief Strategy Officer and Co-Founder, Signicat

44 THE COST OF KYC AND AML

Chau Nguyen, Chairman, Ocular

46 BANKING ON SECURITY: FINANCIAL CRIME, POLITICS, AND THE AGE OF REPUTATION CRISIS

Ron Teicher, Founder and CEO of EverCompliant

48 THE ROLE OF FINTECH IN MAKING FRICTIONLESS CROSS-BORDER TRADE A REALITY

Mario Shiliashki, CEO of Global Payments, PayU

50 ULTIMATE INTELLIGENCE – AUGMENTING THE CHEMISTRY BETWEEN PEOPLE, TECHNOLOGY AND CULTURE

Shawn Rogers, Senior Director of Analytic Strategy, TIBCO Software



Upgrade
to hybrid advisory
processes to serve
the new type of investors
- become part
of the Dorsum Wealth
Management Ecosystem.



My Wealth is a brand new Wealth Management mobile app

which serves the needs of both existing and new generation of customers with adaptive UX. It enables the customers to understand the composition of their portfolio and how it changed over the past. It creates a never before seen seamless communication platform between the customer and the financial advisor. It allows customers to review their portfolio and easy invest within a few taps. It has an emphasis on the education of the customers with the help of the gamification elements and the education marketplace toolkit.

www.dorsum.eu/mywealth

HISTORY REPEATING ITSELF?

THE GREAT BUNDLING DEBATE

When I hear the word bundle I tend to get catapulted back to my childhood, back to the school playground, when the word 'BUNDLE' was shouted and you ran. You either ran to jump on the poor soul who was about to be bundled or ran away from the scrabbling mob bundling you. Now onto financial services. This story is about whether we are heading to or from (or in fact back to) a good old-fashioned bundle.

The Financial Services playground has experienced a movement towards, then away and then towards bundling in recent years all driven by insurgents. While the majority are scaleups such as Zopa, TransferWise, Robinhood or even Square, some are consumer internet companies such as Amazon and Alibaba (via Ant Financial). Moving from specialism to diversification in the quest for scale. But how do these insurgents make the unit economics stack up?

Bundling since the dawn of banking

In the beginning, banks built out their product offerings akin to 'a supermarket' for all financial needs (within reason). Cross-selling and cross-subsidising were key and banks capitalised on their strength of brand and the consumer and political need for trust. Scale and unit economics could be achieved and large players dominated their domestic markets and grew internationally.

As this trust deteriorated during the financial crisis, alongside a demand for better products and choice, the door opened for startups to offer niche products that were either cheaper or easier to use, leveraging their agility and new technology. By leveraging mobile app stores, open APIs, cloud infrastructures and banking regulation, startups focused on single experiences and markets.

Now we are in the early phases of rebundling as customer acquisition costs have risen, due to increased competition and a desire from customers for contextual and seamless experiences. The advent of more APIs, disruptive technologies like artificial intelligence and the ability to leverage structured and unstructured data is meeting these needs, enabling greater insight into customers.

To combat this increasing competition and customer acquisition costs, growing scale or providing more services to existing customer base become essential for insurgent survival.

New models are evolving



The key question is what's next? Is this insurgent model sustainable? In recent years, marketplaces have been enabling a new form of rebundling for those insurgents that have built scale as a niche unbundler. A great example of this is N26 as it connects with niche players to offer a broader range of services to its customers. The best of both worlds if the commercial model can stack up!

To bundle or not to bundle?

There seems to be two business models emerging, firstly those that build their own product capabilities themselves, largely traditional banks and some scale ups and then those that build a platform to connect to third parties and take a commission of every product sold to its customers. There are certainly parallels with how app stores operate and in the domain of financial services, Ant Financial, via its Alipay product has managed to achieve this providing a range of products starting with payments and then moving into savings, lending and much more.

At present the driver seems to be scale. The next consideration needs to be whether the unit economics stack up as the costs to acquire customers are increasing and the competitive playground is changing.

Pat Patel,
Global Content Director at Money20/20 for USA, China, Europe and Singapore

He often engages with the leading companies and rising stars within the Tech, Financial Service and Retail sectors – allowing him to get detailed insight into the strategic priorities for companies, current opportunities and challenges facing the market today and tomorrow. He has overall content product responsibility and oversight of four event platforms spanning the world which enables a truly global view.

In his spare time he actively supports the FinTech ecosystem across Europe, from mentoring startups corporate innovation programs to delivering industry insight presentations at events and national FinTech initiatives.



4th Annual

BFC2019 EU DUBLIN
OCT 07-09

DLT AND EMERGING TECH CONFERENCE

10%
DISCOUNT
WITH
CODE FIT10

Redefining Finance through DLT & Emerging Tech

300+
DELEGATES

15+
EXHIBITORS

50+
SPEAKERS

SPONSORS AND PARTNERS

Deloitte.



David Dalton
Partner Consulting
Deloitte



Marley Gray
*Principal Architect - Azure
Blockchain Engineering,
Board of Directors -
Enterprise Ethereum
Alliance, Microsoft*



Mariana Gómez de la Villa
*Global Program Manager
Blockchain*
ING



Marjan Delatinne
*Global Head of
Banking*
Ripple



Robert Wiecko
COO
Dash



Arthur Breitman
Co-Founder
Tezos

Book now with the discount code FIT10 for a 10% discount:

<http://bit.ly/2LQBFhw>

CHALLENGER AND NEOBANKS

The neobank model

Neobanks, or challenger banks have the customer at the very heart of everything they do. This lies in contrast with the traditional high street banks that have developed in a very product centric and inflexible way. Here lies the main differentiation point. Neobanks respond to customer demand and build their offering around this.

Central to this differentiated proposition is the current/checking account with an associated mobile banking app. Having a current account as a starting point means that neobanks can then add building blocks around that so that eventually they end up with a full service offering that meets the demands of clients.

Unlike traditional banks though, neobanks look to use third-party product offerings, recognizing that customers' needs are not always best served by an in-house solution. In this sense, customers benefit from a best of breed customer centric platform ecosystem.

In a dedicated report, Aite¹ defines the neobank differentiated proposition as follows:

- Mobile-centric design
- Purely digital user experience, real-time, 24/7
- Fast digital onboarding
- Use of new technology, e.g., voice recognition, biometrics, AI decision software
- Direct “social media style” feedback from customers, including ratings and product improvements
- Viral marketing and gamification
- Integrations with transportation, insurance, robo-advisory, social networks, etc.
- Competitive and transparent pricing

Growth strategy

A very modern ergonomic digital platform that provides what customers need is the central tenant to this. For that reason, many neobanks look first to acquire customers and build out from that.

Research from Marcin Mazurek, ‘The Arms Race Among European Banking Challengers Accelerates’, shows that the top seven European neobanks have attracted 8 million customers within a period of 3 years. By 2021, they are



¹ Aite. Neobanks: Banking on the Digital Experience: <https://aitegroup.com/neobanks-banking-digital-experience>



Mary Connor
Director, Product Management, Retail Banking, Finastra

Originally from Dublin, but based in the UK, Mary has been involved with Banking and Banking technology all of her career. Early on, Mary worked for Bank of Ireland (Dublin) and Citibank (London). She has worked as an independent consultant at Fujitsu and a private bank in London. She has been with Finastra on and off for over 20 years and during that time has worked in many countries and areas of the business including training, consultancy, project management and sales; at one point looking after Finastra's 2 largest clients in Europe. Mary's current focus is on Finastra's next generation core banking and working across the business to push forward on innovation in this area.

expected to grow their customer base to some 27 million.

This is an evolutionary process. As the customer base grows then direct income and distribution incomes should build profitability. It comes as no surprise that many neobanks run on VC money for at least three or four years while they acquire customers and build out their proposition, therefore deepening and widening their income possibilities. The Mazurek research also said that the top banks have also received US\$ 1.8 billion in funding, but that monetization still seems to be a distant prospect.

The Aite research found that future profitability will come from:

- **Interchange fees** received on prepaid/debit card transactions
- **Customer fees**
 - Premium account subscription fees
 - Small business banking subscription fees
 - Transaction fees, e.g., ATM charges, card delivery fee
- **Commissions** received from distribution partners e.g., insurance, loans, money transfers (market place model)
- **Net interest income (NII):** balance sheet lending such as overdrafts, personal loans, small business loans
- **Cross-sell income** of other banking services such as investments, mortgages, insurance, and personal financial management.
- **Transaction banking income:** fees from offering the neobank's technology platform to other financial institutions e.g., access to clearing systems

Where does this leave traditional banks?

The high street banks need to fight back from the 'banking is broken' line that the neobanks are pushing.

A neobank's entire proposition is built around being customer centric and having platforms that are extremely agile and scalable. Such platforms can deliver a seamless and guided user experience. These platforms are cloud enabled and are offered as a SaaS model, meaning total cost of ownership is low.

This is the polar opposite of what established banks are offering; with product centric structures and mostly

archaic technology stacks that are inflexible and costly to maintain.

Partnership

In short, each has something the other wants; be that the customer base that neobanks want, or the modern technology stack that traditional banks want.

The Aite research said of this: "Partnerships between neobanks and large financial institutions can benefit both parties. Given their strengths and weaknesses, they appear to be natural partners rather than competitors."

No surprise therefore that we are starting to see the two come together in the form of partnerships and potentially acquisition. This is a common sense evolution.

Research by Mastercard, "European Digital Banking Study", in June 2017, found that despite widespread familiarity with online/mobile banking generally, only 16% of European consumers said they considered changing to a digital bank during the next 12 months. Germans were most ready to switch (27%), while the propensity to switch was lowest in the Netherlands and Sweden.

Traditional banks come with brand recognition, trust and a full and established service offering. They have compliance expertise as well as access to capital and resources.

Neobanks bring not just the technology and platform, they also bring their own products and third-party services to differentiate themselves from traditional banks and even expand their customer base by making it appeal to previously underserved segments.

With the advent of open banking and published APIs, this is becoming more apparent. Neobanks have the technology and capabilities to build a best of breed ecosystem that appeals to their specific customer base and with the flexibility to respond to customer demands.

However, the odds are not stacked totally in favor of neobanks. When open banking matures, it will be possible for third-party providers to build a digital front-end on top of the existing banking infrastructure – providing an alternative to the neobank proposition. The neobank would effectively become a third-party service provider

enabling a service layer provided by the third-party Fintech.

How should Finastra respond?

There is a great opportunity for vendors like Finastra to develop software for new banks. Although there are advantages to working in-house, notably independence and control, the industry has passed the stage where innovating in-house is a viable proposition. The race is towards having a fully functional digital platform that can instantly deliver and enable banks to be more customer centric.

Development from scratch in a highly regulated environment is difficult and has long lead times. In addition, an in-house approach often has an emphasis on a go-live date which sometimes mean that things are rushed and subsequently need changing at a later date. In-house also requires continual investment and expertise, unlike a SaaS model, where the vendor is responsible for maintenance and upgrades.

The Aite research found that: "Commercially available digital banking solutions have reached a stage of maturity and sophistication that will be hard to match by "greenfield" in-house development. Additionally, these digital solutions are easy to integrate with existing bank processes and systems via open APIs."

For these reasons, neobanks are open to the prospect of deploying software from proven and trusted providers. There is a real demand to have the expertise of established vendors on board. Aite expects that new ventures will rely on third-party vendors rather than in-house development.

The opportunities are especially rife in emerging markets where more and more large banks are spinning off digital satellites, and neobanks are getting traction outside Europe, e.g., in the US and in particular in Asia, where the banking infrastructure is much less developed. There is a lack of expertise about what works and what doesn't and how to innovate to offer the very best customer experience whilst maximizing income opportunities. Having something that is easy to use, scalable, agile, totally digital and compatible with an emerging bank infrastructure is going to be a game changer for any bank wishing to operate in these regions.



OPEN

for innovation

It's time for a new way to write, deploy and consume financial software. At Finastra we've done just that, by developing a platform that's open, secure and agile. It lets you integrate new technology seamlessly – bringing new products to market more quickly and with a better customer experience.

As we say, it's innovation with unlimited potential.

(THE FUTURE OF
FINANCE IS OPEN

Join us at finastra.com

SEIZING THE OPEN BANKING OPPORTUNITY

Data-driven innovation is transforming the banking sector. EU's second Payment Service Directive (PSD2) and the General Data Protection Regulation (GDPR), both opens up and protects consumer data. Banks must be better than challenger banks, fintech and social media giants at innovating through the use of customer financial data. At the same time, banks must work harder than ever to build trust and a strong value proposition so that customers consent to a data-led relationship in 2019.

The open banking landscape

The seismic regulatory events of 2018 changed the face of banking. The open banking revolution, sparked by new data laws, forced banks to up their game. Innovative use of customer financial data and select partnership is now key if banks are to survive and prosper.

PSD2 allows consumers to authorise third-party providers to access account and transaction data and authorise payments from their accounts. PSD2 is driving 'open banking', whereby third-party developers can now build applications and services using Open APIs. These interfaces enable them to access a customer's data via the bank's API. All financial Institutions

were required to have any API solutions available for external testing by the end of March 2019. By the end of September 2019 all companies within the EU must comply with PSD2's Regulatory Technical Standard (RTS).

The EU's data protection regulations (GDPR) came into force in May 2018, giving individuals more control over their personal data than ever before. Banks that can transform that from CapEx to investment in data innovation will be those that succeed in the post-PSD2 and GDPR world.

Banks face a real challenge aligning their response to GDPR's demands for tighter data protection with the PSD2 drive to open banking. Any regulated party who obtains user consent to access their data, whether that is an established bank or a start-up, can begin to provide services, blurring the lines between banks and third-party providers and driving competition in the banking sector.

Emerging opportunities

According to the London based publishing and intelligence company, Compelo, an estimated 61 million bank accounts remained idle in the UK as consumers did not close their account but switched

their main banking activities to challenger banks. As a result, traditional banks are losing valuable consumer spending data, instead just seeing “£500 transferred” to Monzo, Revolut or another challenger.

A number of entrants, ranging from fintechs to app developers, are providing standalone personal finance management (PFM) apps, such as Money Dashboard, Yolt, Emma, Mint and YNAB. PFM services have moved beyond simply tracking and categorising spend and represent an opportunity to offer consumers payment, loan and mortgage services that are a substantial portion of bank’s profits. Banks have met this challenge by releasing their own apps or going into partnership with providers who can help with this. Apps that are integrated with the full banking experience provide stiff competition to standalone PFM apps.

While technology giants such as Apple and Amazon were the biggest threat five years ago, in 2018 when PWC asked retail banks, ‘Which non-traditional entrants to the retail banking industry will be your company’s biggest competition in the years to 2020?’, ‘payment players’ were cited as the biggest threat². More than half (53%) of retail bank respondents said that ‘payment players’ such as PayPal, Alipay, Apple Pay, Square, Ripple, WorldPay, Visa and Faster Payments represented the greatest threat to their business.

By contrast, Neo Banks (Starling, N26, Fidor, FiveDegrees, Monzo), technology disruptors (Google, Facebook, Alibaba, Microsoft, Apple) and peer to peer lenders were viewed very similarly when it came to posing the biggest competitive threat, each cited as a threat by 28% or 29% of respondents.

Competition is coming from all sides

New financial ecosystems continue to emerge. The recent partnership between Apple and Goldman Sachs to provide Apple Card, a consumer credit card, has created an entirely new ‘found money’ ecosystem based on open banking. When the consumer uses the card to make a payment, they receive a percentage cashback that goes straight on to their Apple Pay card. As with previous cashback payment cards, Apple receives cashback from the merchant, which is passed to the card holder. What is new is that Apple also earns income from the

‘interchange’, the part of the merchant fee that the card issuer, Goldman Sachs, collects from the merchant.

However, when the consumer uses the card to buy Apple products (or products sold by so-called special partner merchants), Apple pays no interchange fee, saving 2%. This way, it can make it very attractive for consumers using the card to buy its own products by offering discount incentives.

This is a global playing field. Challengers from Asia – Tencent, Alibaba and WeChat – are gaining increasing traction in Europe as Chinese tourists demand these forms of payments abroad. Meanwhile, Monzo, Revolut and lately N26 have their sights set on the US market.

Forward-thinking banks see the opportunity in open banking

All this represents real opportunities for the banking sector. Banks are well positioned to compete, armed with a long-established customer base, trust and a banking licence, all of which put them ahead of new entrants in the starting grid. In fact, forward-thinking banks can use the emergence of open banking as an opportunity to strengthen existing relationships. Capgemini research found that 67% of consumers trust their bank to look after their data – a level of trust higher than any other sector. But banks must continue to build trust – 48% of retail banking customers stated that security is their biggest concern with open banking.

Own the customer interaction

Open banking will be won and lost in the field of data-driven intelligence, so banks are trying to capture as much data as possible in order to provide the best services. The end goal is to own the customer interaction, whether that be with the bank’s own products or through the bank’s fintech partner – with the bank remaining the main brand and interaction point.

How to win in the open banking environment

Meniga has recently published an Insight Paper which focuses on Open Banking. Feel free to download it on www.meniga.com



Georg Ludviksson,
CEO & Co-Founder, Meniga

Serial entrepreneur Georg Ludviksson co-founded Meniga in 2009. Georg is passionate about innovation at the intersection of technology and finance and started Meniga in the wake of the global financial crisis to help people better manage their finances. Georg has over 20 years of experience founding, building and leading software companies with a global ambition, including enterprise mobility company Dimon Software in 1998 and social investing site UpDown.Com in Boston in 2007.

Georg holds an MBA degree from Harvard Business School with emphasis on Entrepreneurship and Finance. He also holds a BS degree in software engineering from the University of Iceland.



TIER TWO BANKS: IS THERE A FAST- TRACK TO A CHALLENGER UX?

Absolutely, says Lars Sandtorv, CEO, MeaWallet. By tapping into specialist tokenization platforms resource-strapped incumbent banks have a chance to turn the tables on the challenger banks, delivering a rival UX that creates new revenues and reduces customer attrition.

It's widely acknowledged that incumbent banks are struggling to keep pace with digitalization. As a result, they have given oxygen to the alternative payment systems and lightweight, fast moving challenger banks that now inhabit the space they have failed to fill. These players have already gained traction and now threaten to extend their lead. The convenient and ultra-flexible, app-based user experiences they deliver continue to capture headlines and command a following of digitally literate end users that is growing faster as each day passes.

Blaming what it dubs the 'friction endemic in almost every legacy payment system', a recent report from Deloitte¹ reveals quite how quickly users are moving away from using incumbent bank cards to pay for goods. PayPal already has 250 million users. Apple Pay is on track to reach 200 million users by 2020. By then the global transaction value of mobile payment apps is expected to reach \$14 trillion². Barely a month goes by without news of the launch of yet another digital-only challenger bank.

Prominent among the disruptors are the OEM Pays. Google Pay, Apple Pay, and Samsung Pay – for example – have blossomed and

continue to grow, with key players now serving between 25 million and 85 million users.

The challenges facing banks are particularly serious in Europe, where the fintech scene is flourishing. In a recent keynote speech³, European Central Bank vice-president Luis de Guindos suggested that, in parallel with meeting structural challenges, the continent's banks must face down growing competition from the sector: "increased competition in lending, investments and payments is bound to increase pressure on retail banking revenues."

Can banks respond? Particularly challenged are those tier two and tier three banks that have neither the resources nor the technical skills to pump into digital innovation, integration of third-party technologies or the development of their own proprietary offerings.

Better together

Fortunately, as the consumer-facing alternative payment systems and challenger banks have been evolving, so too have the bank-facing third party service providers. Based around the smart use of tokenization, this new breed of partner provides established banks with an easy-to-integrate platform of up-to-the-minute mobile and card payment functionality that can be easily integrated with their existing services. This means that these banks can sidestep the costly and time-consuming development and integration that conventionally accompanies the creation of such capabilities and

¹ 2019 Banking and Capital Markets Outlook

² The rise of digital and mobile wallet: Global usage statistics from 2018

³ Euro Area Banking Sector – Current Challenges



Lars Sandtorv,
Chief Executive Officer, MeaWallet

With over 20 years' experience in the field of technological innovation, Lars Sandtorv is the Founder and CEO of MeaWallet. After setting up the company in 2013, Lars has been a driving force behind establishing MeaWallet as one of Europe's leading companies within mobile payments.

MeaWallet develops globally recognised tokenization technologies which serve banks and card issuers through a proprietary, platform agnostic product suite. The company is a Mastercard Engage Partner, part of the Visa Token Service Ready Program and an American Express GNS partner for Amex Pay. MeaWallet's Digital Payment Platform enables a range of digital payment services including tokenization (MDES, VTS, Amex TS), OEM Pays and secure remote commerce (SRC). Built to support any payment scheme, the platform enables card digitization to any wallet application and wearable device for mobile and digital payments, all through a single connection. The platform reduces time-to-market, simplifies integration and reduces risks for card issuers.

instead focus on designing products that meet their customers' specific needs, safe in the knowledge that both the customer experience and myriad technical security requirements mandated by the schemes and OEM Pays are taken care of.

By combining OEM Pay functionality with additional features like EMV® Secure Remote Commerce (SRC), tokenization and token management facilities, banks can provide customers with a convenient and flexible end-user experience that genuinely rivals that of the challenger banks.

So, what individual benefits do these capabilities bring to the table?

- **Payment-enabled bank apps**

By enabling a mobile banking app with wallet functionalities, customers can make in-store payments. This provides the flexibility to not only manage finances in an app, but make payments in the same breath.

- **Issued card to OEM Pays**

Connecting a banking app to OEM Pays gives banks the potential to grow the customer base by providing a broader, more flexible solution in allowing consumers which wallet they'd prefer to use.

- **SRC enabled payments**

SRC is the next step in eCommerce that will enhance both security and user experience in online shopping. Customer benefits include a frictionless shopping experience via a reduced need for entering card and shipping information.

- **Greater customer control with a tokenized app**

Tokenization has become the new and modern standard to secure, provision and store card data to mobile, IoT devices and online merchants. With it, customers have the ability to enable push

provisioning and manage tokens across multiple card schemes directly from the app.

By improving functionality and increasing app usage, banks can improve customer loyalty and reduce attrition. This has knock-on benefits: improved cross-selling opportunities, keeps the bank's brand front and centre in the mind of its customers, and creates opportunities for new, profitable revenue streams from the newly available features.

Time is of the essence

These challenges and opportunities coincide with the arrival of open banking regulation and associated innovations in bank direct payments. In time, these will significantly impact how banks generate income.

PSD2 may improve consumer rights in certain areas – it will also improve security – but it will also enable third-party access to previously exclusive account information and create an environment for new payment and account services that piggyback on the bank's assets.

With the bulk of legislation coming into effect in September 2019, banks need to move now to shore up their own offerings on the anticipation of increased competition in the near future.

With time running out, taking a few painless steps now to bring their digital services up to date will serve banks well in the future. Tomorrow's market for digital financial services market is heating up and the quality of user experience will be a key battleground in the fight to win - and retain - customers.

As digital transformation continues to proliferate, financial services players such as banks and financial institutions, would be wise to look to key technology providers in the industry, in helping them to minimize the impact of fraud.

We interviewed Nicolas Muhadri, CEO StreamMind, a high-tech company providing secure interbank transactional messaging, instant payments, verification and fraud prevention, to discuss his thoughts on the recent fraud issues in the industry:

“Fraud, being one of the major security implications of digital innovation, is becoming an increasing issue for the financial services industry. Bank transfer fraud, in particular, has entered the media spotlight during the past couple of years.”

Victims have lost vast amounts of their personal savings through such schemes, with little to no legal backing when it comes to claiming damages for their losses.

At StreamMind, we have been working on solutions for erroneous transactions taking place online. Our anti-fraud solution, Lucy, is the first of its kind, as it allows enterprises to check, in seconds, that the bank details of their suppliers match the name of who they’re paying.

Bank transfer fraud relies on the switching of bank details of named suppliers, to their own account, which is incredibly different to detect as there is no way to validate that the name matches the bank account, without additional overlaying software.

Previously, companies have incurred huge financial losses, with no reimbursement available, as there is no legislation to support a fraud claim if you were to issue the payment to the wrong individual – you are considered liable for the error.

With our network of hundreds of banks, we can now offer a secure solution to enterprises and banks for all types of transactions – national, international and interbank. We already have the technology in place, and we have built the software to connect banks and customers.

StreamMind is also the software editor of MoneyRoad, the new Digital payments app, which is compliant with the Single Euro Payments Area, the new industry standard format for cross-border European bank transfers. It is available on tablet and mobile, on the web, as an API, and is also completely customisable.”

With new data released from banking trade body, UK Finance, it has been revealed that incidents of authorised ‘push’ payment scams reached 84,624 in 2018, with total losses of £354.3 million. It was also revealed that in the second half of 2018, £209m was lost in bank transfer fraud, compared to the £145m lost in the first half of the year.

Banks are clubbing together to respond to this challenge: in February this year, several of the leading industry banks signed up to a new code involving a reimbursement scheme, showing further interest to this area, and following the super-complaint made by Which? in 2016, ‘Consumer safeguards in the market for push payments’.

Why has transfer fraud increased?

In 2018, there were a significant number of high-profile data breaches, which resulted in large amounts of consumer data being compromised.

Data collected through fraudulent means can be used many years after the event has taken place, and can be used to facilitate deception scams against small companies and consumers, making them highly convincing and far more difficult to guard against.

“The fact is that criminals are becoming smarter, so we [technology players] and the banks, retail players, and so on, combined, need to become even smarter, as a result.

The increased use of data has led to an increase in scams fueled by an authenticity and accuracy that just wasn’t there before.

Criminals can use personal and financial data to defraud customers and trick them into thinking the request is genuine, by posing as HMRC, or DVLA, or impersonating a banking site - all with access to their personal data to further validate their claims.”

StreamMind is currently working with the largest banks across France, and, as they are already classed as a leader in this arena in France, they are well-versed to offer first-rate solutions for the European sector as whole:

“We are leading in the market and expanding globally. Europe is the first area to target on our roadmap, and the beauty of our product is that it’s already succeeding in a European territory, and therefore our clients know it is ready to roll out into other European countries as it has been tested and proven to work.

We are really looking forward to discussing our proposition in more detail at Money20/20 this year, and meeting with banks, financial institutions and enterprises to show them how they can avoid fraud easily, and in seconds, with our solution, Lucy.”

Managing the fraud risk with StreamMind’s ‘Lucy’

“Our mission is to empower any enterprise with the tools to adapt to the demands of digital transformation securely. Typically, innovation isn’t considered synonymous with security in our industry, and that’s a stigma we really want to challenge. We believe the two can come hand in hand, and they have to in order to guard against the fraud issue effectively.

We’re certain we can help with many aspects of the fraud dynamic faced by banks and financial institutions – particularly in long-distance payments, which account for 73% of fraudulent payments.

As we already partner with several hundred of the largest banks, who are already connected to our technology, we see our solution being as secure and effective for international payments, as for domestic transactions.”

StreamMind is currently a leading high-tech player in France, and was established in 2008. The company specializes in transactional and messaging software solutions, with the aim of building software solutions that provide both robust and agile, as well as, simple, adaptable and scalable solutions for enterprises.

Their TIME™ technology is the product of ten years of research and development. StreamMind built also the first interbank network totally opened and highly secured in cooperation with the major French banks (Caisse d’Epargne, Crédit Mutuel, CIC, Crédit Agricole, BNP, and Société Générale) and several leaders in the information technology sector (SUN Microsystems, HP and IBM).

¹ Where the victim initiates the transaction from their own bank account, having been tricked by the scammer through a deception scam.

Nicolas Muhadri,
Chief Executive Officer,
StreamMind

THE RISE IN BANK TRANSFER FRAUD: CAN YOU AFFORD TO LOSE OUT?

CAN YOU AFFORD FRAUD?

£354 million lost in bank transfer scams in 2018, only £83m ever recovered.

Start avoiding fraud and errors today. Streammind's verification software, LUCY, allows you to validate and match identity with bank account numbers and sort codes.

Lucy processes 2 million verifications in just 30 seconds.

What can you do in 30 seconds?

Visit our website www.streammind.com

**Join us at
Money20/20
Booth K20-7**

About StreamMind:

StreamMind is a leading technology provider, that allows both corporate financial institutions and enterprises to adapt and protect themselves in the fast-paced digital transformation. StreamMind has over 10 years history supporting the biggest financial institutions in Europe with secure interbank transactional messaging, instant payments, verification and fraud prevention. StreamMind is the lead software editor for the SEPAmail network and work with over 400 banks, making it the largest interbank network.

PSD2 APIs: ARE YOU READY TO RESPOND TO THE NEW FRAUD THREATS?

In the EU, Payment Service Providers (PSPs) were supposed to have their Payment Services Directive (PSD2) APIs available for external testing by May 14, but only 59% of FIs actually achieved this according to at least one survey. The race is now on to hit the September 14th live date for these APIs, along with the additional requirement of Strong Customer Authentication (SCA). This means some serious catch-up for those who missed the first benchmark.

With these new APIs, come new fraud threats. PSD2 and Open Banking will start to have a greater effect on fraud, for customers, financial institutions and the fraudsters. However, the full impact may take longer to materialise. Whilst there are some Payment Initiation Services (PIS) available, with Yolt in Beta, Ayden and IATA pay being demoed, the killer use cases for using PIS providers are yet to be in place.

So what are these threats?

Firstly, Open Banking is another vector for social engineering, a way to confuse customers into handing over credentials or data to fraudsters. This certainly muddies the clear message that banks previously sent to customers, which was not to share your bank credentials with anyone.

However, there are more complex threats than simple social engineering. It's perfectly possible we will see either an outright fraudulent Third-Party Provider (TPP) fronting themselves as the financial institution, or one that is hacked or socially engineered in some fashion. And this could result in fraudulent payments, account takeover (ACTO) and even more data compromises to facilitate ID Theft.

Open Banking will also have a direct negative impact on a financial institution's ability to undertake fraud profiling. This is because, instead of having full control of the end-to-end journey via their website or app, the FI will only see the customer's

endpoint (e.g. laptop or, mobile device) at one or two points in the journey. This makes it much harder to manage as they move from continuous authentication to a point-in-time model.

Further, we will see a shift in transaction types, away from cards for e-commerce transactions (potentially at POS too), to increased real-time push payments for purchases at merchants. This shift will impact the fraud profiling models used by FI's and will take time for this to catch up with the highly mature models currently in place for both cards and payments over the different rails today.

What all these threats create are the following problems:

- Increase the overall fraud in the system
- Make frauds harder to spot
- Place additional costs on traditional FIs to manage fraud
- Make it more difficult for banks to reclaim fraud from other parties in the ecosystem

Unlike card networks, with clear rules on liability and methods for issuers to easily reclaim funds from other participants, e.g. merchants, there is no clear model to do this with Open Banking. Financial institutions are going to be the customer's first port of call when a fraud has occurred, and in the EU FIs will be obliged to refund unauthorised transactions immediately, even where this occurred through a TPP and increasing the overheads on contact centers.

What Can the Industry Do to Counter Fraud Threats?

Firstly, FIs should work together as an industry, including the new Third-Party Providers (TPP)s, to provide clear education and messaging to the customer so that they are aware of the scams to watch out for. This should include ensuring there is an independent method of customers being able to identify genuine TPPs and those that are authorised, where appropriate for example in the EU.

NICE · ACTIMIZE

Robert Tharle,
Fraud and Authentication Subject Matter Expert,
NICE Actimize

Rob Tharle is responsible for providing thought leadership on industry trends, challenges and opportunities. Prior to joining NICE Actimize in 2019, he worked for 17 years in a number of Risk Management and Fraud Prevention roles at both Natwest/RBS and TSB. During that time, Rob gained extensive experience with the technologies and design of fraud prevention and detection systems including application fraud, Apple and Google Pay, online and mobile banking.



FIs should support provide APIs, even where they are not under regulatory pressure to do so, e.g. non-payment accounts in the EU. This should be replacing screen scrapping rather than just blocking these services. This will help reduce the social engineering aspects around credential sharing as well as provide a new source of income.

There should be encouragement for TPPs to implement similar layered fraud prevention systems as traditional FIs, e.g. device profiling, malware detection, behavioural biometrics at customer endpoints, along with sophisticated fraud profiling and advanced analytics.

FIs would also do well not to annoy customers with clearly blanket policies around authentication and have risk-based models for TPPs when undertaking authentication to support a sensible customer message.

This should include sharing best practices and data in the fraud and security space to reduce fraud in the overall ecosystem. This can be accomplished via industry bodies or via consortiums of the fraud solutions suppliers. Such solutions might include such things as details of known bad devices or known mule accounts. This effort should be further expanded to build out clear liability models and processes to encourage best practice and reduce costs in the overall system.

Build Out Fraud Profiling Platforms

What are the key actions for financial institutions? Firstly, FIs should build out their fraud profiling platforms to treat Open Banking transactions as a separate channel, whilst ensuring the system sees as many transactions (preferably all) the customer makes, as possible. This means building bespoke models and journeys for these new transaction types, while preventing the creation of silos.

Additionally, FIs should increase the data available to these systems to include device profiling, malware detection and behavioral

biometrics, as well as data on the TPPs themselves. In the EU, they should also consider using PSD2 as a legal justification under GDPR to capture customer location and other data to aid fraud prevention.

Utilising the PSD2 Strong Customer Authentication (SCA) exemptions will also be important, both in reducing friction for customers, but also to ensure the full weight of fraud controls and referrals fall on the highest risk transactions, improving efficiency and reducing costs.

Fraud profiling should also be expanded to cover the TPPs themselves, e.g. 'What risk does this TPP pose based on the behaviour seen?' This should be updated in real time and can then be used within models. It can also be applied to check the certificates validating a TPP's identify and right to offer the services, based on the risk. This will become important when there are hundreds of TPPs, to reduce cost and latency.

To win the battle against new fraud threats, financial institutions will need to have reporting and monitoring of Open Banking transactions in place to provide insight into how they are being used and abused, looking for anomalies along with understanding any new fraud typologies.

Banks and FI's might also consider making good use of Open Banking by becoming TPPs themselves. Many of the UK Banks, such as Lloyds and Barclays, have already started to do this. This could help them identify fraud and reduce false positives, if they can see all of a customer's accounts across the industry. This will also help them to think like a TPP, which will be useful in preventing fraud via TPPs. They should also look at other opportunities from Open Banking, such as becoming a trusted source of identity, to underpin Open Banking.

It is clear there are real fraud issues that must be addressed, but there are also ways to enjoy the benefits that Open Banking has to offer customers and FIs. There are activities individual organisations can do themselves, but all parties in the eco-system should join together to help secure these benefits for all.



embrace the true digital core banking transformation.

We are the fintech engineers.

We combine state-of-the-art technology and sound financial knowledge to create unique digital solutions for today's banks. Future-proof your bank with the right digital core banking platform.

Digital transformation is one of the key challenges for today's banks and financial service providers. For some, switching from legacy systems to a new digital core banking solution looks like a highly complex and costly process. We empower banks to make the digital transformation, leading to stronger customer relationships, greater profits, and lower costs.

More information: [fivedegrees.com](https://www.fivedegrees.com)

five°degrees
the fintech engineers

COLLABORATION THE KEY TO FIGHTING FINANCIAL CRIME

ATM & Cyber Security 2019 is the world's leading conference dedicated to tackling physical and logical ATM crime. Organised by RBR and held annually in London since 2007, the event brings together banks and other ATM deployers to discuss and share best practice on protecting against the latest ATM threats. We caught up with RBR's Gillian Shaw, who is managing the conference agenda, to find out more about the latest security trends and why the fight against financial crime remains at the top of the industry's agenda.

Financial IT: *Can you start by explaining a bit about how ATMs are affected by cybercrime?*

RBR: ATMs are vulnerable to ATM-specific cybercrime either in the form of remote cyber-attacks, when malware such as ATMitch is used to take control of servers to dispense ATM cash or direct malware attacks when criminals use direct access to the ATM to deploy malware such as Ploutus-D. Direct cyber attacks on ATMs are known as "jackpotting" and this threat has been increasing significantly over the past few years. It is particularly dangerous as this sort of attack is quick and inexpensive to execute and because it can empty an ATM within just a few minutes. Cyber security solutions can deal with an array of infrastructural vulnerabilities but ATM hardware and operating systems often remain the weak points. Today, ATMs require the same levels of rolling security provision and upgrading as every other aspect of bank infrastructure.

Financial IT: *What sort of physical attacks are we seeing against ATMs at the moment?*

RBR: ATMs are the perfect target for both conventional thieves and more modern hackers. The most visible attacks are, of course, the violent attacks carried out by organised criminals who use explosives or "ram raid" ATMs with heavy vehicles to extract cash. Explosive attacks, whether by gas or solid explosive, are a rising problem in Europe and in many other parts of the world. Such attacks result in extensive damage and can pose a risk to life. The success rate for ATM physical attacks is alarmingly high and recent data from the European Association for Secure Transactions shows that losses related to these sorts of attacks rose by 16% in Europe in 2018. Collateral damage to equipment or buildings resulting from physical attacks can also be substantial and often exceeds the value of cash stolen.

Financial IT: *What other threats are there against ATMs?*

RBR: The past few years have seen criminals applying their creativity to stealing money from ATMs, with considerable success. ATM skimming attacks, when physical devices are placed in card slots to capture information from swiped cards, have become increasingly sophisticated. "Shimming" is a new variation on this attack that can

steal data from chip-enabled cards in ATMs or point-of-sale machines using a paper-thin insert in the card reader. It's especially dangerous because of how simple the attack is. All thieves need is a few seconds of access to the machine, and the insert can be hard to detect once deployed.

Financial IT: *Turning back to cybercrime, how is the general cyber security threat landscape changing?*

RBR: As the growing number of apps and portals facilitate an increasing number of electronic transactions, they pose a new risk for banks and other financial institutions in terms of cyber security. Banks need also to be very mindful that the threat landscape around insider fraud and social engineering is changing rapidly. Criminals are continually developing new modus operandi to manipulate victims into making security mistakes. Phishing, gathering personal information using deceptive websites and emails, has become an increasingly sophisticated form of cyber attack in recent years and banks need to develop effective education programmes for both clients and employees to counteract this and other similar threats.

Financial IT: *What can the industry do to respond to evolving ATM and cybercrime threats?*

RBR: Banks and ATM deployers have the responsibility to constantly monitor threat risks. This should involve a holistic approach to how vulnerabilities are identified. They must continue to invest in technical cyber defence. However, they also need to develop broader strategies to engage with governments, other banks, their clients and the general public. This will be all the more true as fintech develops ever more complicated digital systems that increase interconnectedness, and therefore vulnerabilities.

Financial IT: *How can security events such as ATM and Cyber Security 2019 help in the fight against financial crime?*

RBR: It is only by collaboration between stakeholders that the industry can keep one step ahead of criminals. ATM & Cyber Security 2019 brings together security professionals from around the world to share their knowledge and discuss best practice with their industry peers. In addition to the two-day speaker programme of innovative bank case studies and thought leadership, delegates also have the opportunity to explore the latest ATM and cyber security solutions and get advice from industry experts.

ATM & Cyber Security 2019 will be held at the Park Plaza Victoria Hotel in London, on 8th and 9th October. If you would like to get involved as a speaker, exhibitor or delegate, please contact Gillian Shaw at RBR by emailing gillian.shaw@rbrlondon.com.



Meet our conference partners

RBR events bring together the world's leading banks and industry experts – join our growing partner lineup...



learn | explore | network
www.rbrlondon.com/conferences



Yinglian Xie,
CEO and Co-Founder, DataVisor

Yinglian Xie is the CEO and Co-Founder of DataVisor. Her path to this role began with Carnegie Mellon University's computer science department, where she earned my Ph.D.—her thesis was on network security and doing large scale detection and forensic analysis. After completing her degree, she joined Microsoft Research in Silicon Valley, and she started moving into application levels of all kinds, working on preventing fraud and abuse, and other malicious actions impacting consumer-facing groups. At the end of 2013, Dr.Xie and her Co-Founder Fang Yu decided to try something really groundbreaking. After seeing so many different kinds of fraud and abuse issues across different industries, she wanted to build something new; something comprehensive and transformative; So, she set out to build a company, DataVisor that can take cutting edge research and apply it to real-world problems at the highest scale.

DATAVISOR – EMBRACING PROACTIVE APPROACH TO FRAUD MANAGEMENT

An Interview with Yinglian Xie, CEO and Co-Founder of DataVisor.

Financial IT: *Can you tell us more about your background and career path that brought you to launching DataVisor?*

Yinglian Xie: I am the CEO and Co-Founder of DataVisor. My path to this role began with Carnegie Mellon University's computer science department, where I earned my PhD—my thesis was on network security and doing large scale detection and forensic analysis. After completing my degree, I joined Microsoft Research in Silicon Valley, and I started moving into application levels of all kinds, working on preventing fraud and abuse, and other malicious actions impacting consumer-facing groups.

I was thrilled to be contributing in this field. The digital era was evolving so rapidly, and I was excited to be facing and solving so many new challenges. Suddenly, there were hundreds of millions of users online, creating and sharing content, making and receiving payments, buying and selling goods. The sophistication was incredible, but at the same time, very complex problems were emerging. As creative as the digital innovators were, fraud was getting creative as well, and fraudsters had the advantage of not having to follow the rules. This was the challenge that motivated me—how can we create a real-time, highly accurate solution for fraud attacks that get more sophisticated seemingly by the minute? How can we solve for all the different use cases, when fraud is becoming so diverse, and so omnivorous? Algorithms alone weren't the answer. We needed a working solution that could be applied everywhere.

At the end of 2013, my Co-Founder Fang Yu and I decided to try something really groundbreaking. After seeing so many different kinds of fraud and abuse issues across different industries, we wanted to build something new; something comprehensive and transformative; something that could be applied more widely than anything else we'd seen.

To do this, we had to integrate theory and practice. You can think of it like cooking. As a researcher, I came from the recipe side. We were making great recipes, but for great food, you need great ingredients, and it has to all work together to become a great dish. So, we set out to build a company that can take

cutting edge research and apply it to real-world problems at the highest scale.

Financial IT: *What is special about DataVisor and how it helps to stand out among its competitors?*

Yinglian Xie: The fact that fraud tactics do change so rapidly is why companies like DataVisor embrace a more proactive approach to fraud management. If you are only keeping up with fraud, you are already behind. Both rules-based and supervised machine learning-based approaches are inherently reactive, and as such, can only identify known fraud. So they help, but they can't do everything. To meet emerging threats and prevent fraud before damage occurs, organizations must be able to accurately identify unknown fraud types as well.

Unsupervised Machine Learning (UML) offers fraud teams a new superpower—the ability to deploy highly accurate detection models without the requirement of historical data or pre-existing labels. This approach can feed into an overall strategy that prioritizes holistic analysis and contextual detection. It is important to look at events as a whole as opposed to reacting to them one at a time, and businesses must be empowered to discover the clandestine correlations and patterns that signify fraudulent attacks before they're unleashed.

There are additional advantages to deploying a UML-powered approach, including seamless and rapid integration, actionable results, and early, demonstrable ROI. The ability to deconstruct events within fraud attacks, investigate complicated cases with detailed detection reason codes, and view correlated activities across all accounts, is the key to staying ahead of fraud, and preventing damage before it happens.

Financial IT: *What are the emerging trends you foresee in the industry today and how do you address these new challenges?*

Yinglian Xie: Sophistication. Complexity. Scale. These are the challenges we face, and the consequences of failing to do so are getting more and more severe. If you don't believe in AI, then you may not believe it's possible to keep up with the new fraud

attacks—they're so cleverly disguised, they move and adapt so fast, and just as soon as a new technology emerges, it seems that fraudsters are using it against us.

Bots are a perfect example of this. The introduction of bots to the fraud equation means organizations now have to contend with an entirely new scale of fraud. The larger the fraud ring, the more likely bots are involved, and the more that bots are involved, the harder it is to detect the fraud, because the hallmarks of a bot attack can change very rapidly.

Bot-powered fraud is supremely challenging to detect, and even harder to prevent. Attacks are often massive in scale and can adapt very rapidly. So the question isn't whether your organization can afford to invest in prevention. The question is, can you afford not to?

To defeat bot attacks, you need to meet scale with scale. DataVisor's advanced fraud management solutions detect even the largest, most complex, most cleverly disguised attacks. Unrivaled domain expertise informs every feature; proprietary unsupervised machine learning algorithms adapt in real-time; a massively scalable detection engine correlates behavior across users and accounts."

Financial IT: What is next for DataVisor?

Yinglian Xie: One of the most exciting things about our approach—and about the growth DataVisor is experiencing right now—is that as we continue to add so many incredible clients, we're able to optimize our solutions in really powerful ways that directly address challenges specific to different industries. The financial services industry is a perfect example. Application and transaction fraud, account takeover, money

laundering—with DCube, we're empowering financial services companies to proactively detect and prevent exactly those fraud types that are most impacting them. Because of the insights our clients provide us, we're able to provide exactly the tools and capabilities they need, and at the same time, we're promoting a safer and more connected digital world where actionable intelligence can be used to maintain trust, deliver frictionless customer experiences, and protect data.

Financial IT: Can you please tell us more about your participation at Money20/20? What will DataVisor showcase at the conference?

Yinglian Xie: We know from our research that financial institutions are the hardest hit by the most highly-coordinated attacks, so we're very excited to expose them to the power of DCube, and to show them how they'll be able to stay ahead of massive, coordinated attacks by deploying a holistic approach to data analysis. With DCube, we're giving an incredible degree of control to both fraud teams and data scientists, and best of all, we're presenting them with an all-in-one platform where every stakeholder can seamlessly collaborate for maximum efficiency. From data management to feature engineering, DCube gives companies the ability to combine our fraud domain expertise with their organizational expertise to build high-performance models while meeting the demands of transparency and compliance. Financial institutions are ready for this transformation as they strive to remain competitive with the latest technology, and DCube delivers on the promise to prevent fraud before financial and reputational damage occurs.



The Complete Fraud Prevention Platform

Capture Known and Unknown Fraud Early

Manage Enterprise Workflows Efficiently

Analyze Data Holistically

› Application Fraud › Transaction Fraud › Anti-Money Laundering

info@datavisor.com | www.datavisor.com



Financial Operations Made Easy

Allevo provides software solutions that help banks, companies, microfinance and public administration achieve process automation and compliance.



FinTP is a software application for financial institutions. It offers management of real-time payments, liquidity and assets. Its core enables technical integration between various proprietary formats and applications, performs message routing and format conversion, while also ensuring data persistence, protection and archive with advanced reporting capabilities.

FinTP consists of a variety of functional features that make up the core of the application, and additional business and operational features are available, allowing the setup of an environment suited for needs of every customer.

FinTP-Instant connects back-office applications of a bank to the Instant Payments service offered by TransFonD, retrieving payment messages in any format provided by these applications (tables, queues, etc), ensuring their conversion to the ISO 20022 standard and routing them to the Instant Payments System (IPS). Target audience: banks, public administration.



FinTP-Connect is a solution for centralized management of requests initiated by PISP/AISP on behalf of the final customer. It retrieves and processes these requests, transfers them to the Core Banking system, and then returns the responses back to the PISP/AISP. Target audience: banks.

FinOps Suite* is an open source solution for SMEs and corporate treasuries that centralizes financial and treasury operations, consolidates payments, and includes a short-term prediction component for liquidity flows. Target audience: big manufacturers, service providers, small and medium enterprises, payment processors, financial infrastructures, microfinance.



FinTP-Instant

- Instant Payments
- Straight-through processing
- Connection to TransFonD
- Process credit transfer instructions
- Interface via web services
- Timestamp
- Monitoring

FinTP-Connect

- PSD2 compliance
- Centralized request management
- Back-office integration
- TPP identification & validation
- API management integration
- Data analytics
- Access for PISP & AISP

FinOps Suite

- Corporate treasuries
- Payment management
- Reporting
- Reconciliation
- Operational features
- Message routing
- Automation and integration

**FinOps Suite is the business name of the software solution being developed as part of the Treasure Open Source Software (TOSS) project. This project is co-financed by the European Regional Development Fund under the Competitiveness Operational Programme 2014-2020, Priority Axis 2 "Information and Communications Technology (ICT) for a competitive digital economy".*

Ioana Guiman,
Business Development & Managing
Partner, Allevo

Ioana has been on the board of Allevo since 2016, focusing on strategizing and finding new business opportunities in financial services.

Passionate about solving financial inclusion and driving more transparency in banking, she is also an advocate of open source software, responsible solution design and business ethics. Having a technical background in computer science, Ioana is with Allevo since 2003, covering various roles: software developer, solution designer, system engineer. With an open heart for finding custom solutions to very specific customer problems, she is always keen to ensure customers get excellence, both in terms of products and services. Always on the lookout for the next best thing, keeping a close network of financial services experts, FinTechs and key players, to benefit from their insights and know-how.



FINANCIAL OPERATIONS
MADE EASY

Allevo is one of the players active in the financial services space for the past 20 years. What’s different from most competitors is that Allevo is a privately owned company coming from an emergent market, Romania. Although it may not seem much, having to compete with companies that have access to far richer resources is not an easy game to play.

In this context, Allevo has proven constant agility in designing new software solutions that address issues of financial services institutions. Notable innovations include the design of an application that achieves integration and financial process automation, an application for achieving accounts reconciliation, an application that manages the disbursement and loan repayment flows for microfinance, an application that automates the financial flows of corporate treasury, an application that enables banks and FinTechs to operate in an Open Banking setup, and last, but not least, the open source business model.

The solution portfolio allows Allevo to address a broad selection of players, ranging from banks, to companies, microfinance, public administration, money transfer operators, credit institutions and so on.

The last couple of years have been very intense. One major area of focus was finalizing the open banking solution that allows banks to achieve compliance to provisions of PSD2. The second was the implementation of the TOSS project, a project co-financed by the European Regional Development Fund under the Competitiveness Operational Programme 2014-2020, Priority Axis 2 “Information and Communications Technology (ICT) for a competitive digital economy”.

FinTP-Connect was delivered in 2018 in two proofs of concept to two banks in Romania, allowing them to test early an open banking architecture, the flows behind, security concerns included. FinTP-Connect is just the starting point to enabling a bank to communicate with partners, customers or competitors even in a standard way, via APIs. The major benefit of such an implementation is the step towards interoperability, something Allevo has been advocating for for a very long time.

The software solution developed as part of the project targets SMEs and corporate treasuries. The project enables the use of IT and communication, reducing cost and processing time for the processing of financial operations of companies. Possible extensions include

the relationship of the corporate with its business or individual customers and the provision of added value financial services.

FinOps Suite¹ is the business name of the software solution being developed as part of the Treasure Open Source Software (TOSS) project.

The main objective of the project is the growth of competitiveness of Allevo as a company by developing an innovative open source application. This application processes financial transactions for SMEs and corporate treasuries and is distributed under the GPLv3 open source license via the fintp.org portal.

MORE SPECIFIC OBJECTIVES ARE:

1. The development of the FinTPc application for processing financial transactions, aimed for SMEs and corporate treasuries
2. Annual turnover growth by EUR 200,000 in the first 3 years after finalizing the project
3. Gaining up to 23 new internal and external users of the application, over the first 3 years since the implementation of the project.

Although it does not sound too complicated, a lot of effort has been placed in developing this application and delivering the other components of the project.

Two such components are the allevo.ro website and the fintp.org website. These have been completely redesigned, not only from a look and feel perspective, but also in terms of content, logic, navigation and features for users.

The software is distributed under the GPL v3 open source license and is also available to members of the EURONEST Regional Innovative Cluster IT&C HUB, that Allevo is proudly a part of.

TARGET AUDIENCE OF THIS PROJECT:

- Big manufacturers (automotive, pharma, and energy industries, among others)
- Service providers (distribution of utilities, distribution of goods, retail chains, and many more)
- Small and medium enterprises that are collaborating with big manufacturers
- Financial transactions processors or third-party service providers for certain financial instruments
- Intra- or inter-sectorial financial infrastructures

FinTP-Instant	FinTP-Connect	FinOps Suite
Instant Payments	PSD2 compliance	Corporate treasuries
Straight-through processing	Centralized request management	Payment management
Connection to TransFonD	Back-office integration	Reporting
Process credit transfer instructions	TPP identification & validation	Reconciliation
Interface via web services	API management integration	Operational features
Timestamp	Data analytics	Message routing
Monitoring	Access for PISP & AISP	Automation and integration

¹ FinOps Suite is the business name of the software solution being developed as part of the Treasure Open Source Software (TOSS) project. This project is co-financed by the European Regional Development Fund under the Competitiveness Operational Programme 2014-2020, Priority Axis 2 “Information and Communications Technology (ICT) for a competitive digital economy”.



HYBRID ADVISORY MODEL: MEETING THE NEEDS OF GENERATION X AND GENERATION Y SAVERS AND INVESTORS

An interview with Imre Rokob, Director of Business Development at Dorsum

Financial IT: Can you tell us a little about Dorsum?

Imre Rokob: Dorsum is an award-winning, innovative investment software vendor with a strong presence in the CEE region. Dorsum was established in 1996. Since that time, our company has grown from a few employees into an organization, with a staff of 300 for delivering integrated investment IT solutions. We have a deep understanding of the objectives of financial institutions within the ever-changing economic environment. Moreover, we are delivering solutions based on the trends of the industry and on the knowledge that we have gathered over the decades. There are more than 90 clients of Dorsum, and we support them by offering unique cooperation throughout the lifecycle of the products, managing expectations in terms of functionality, time and budget.

Financial IT: Please comment on the big changes that you have faced since the company's foundation in 1996.

Imre Rokob: Since our foundation in 1996, innovation has been always the main feature of the company, which has helped us to become a leading software provider in the Central and Eastern European (CEE) region.

Amidst much change, MiFID I and MiFID II have been key developments - affecting not only investors but also banks and wealth managers. Financial institutions have had to deliver new insights and information, yet at precisely the same time that their profit margins have come under downwards pressure.

The next big thing will be hybrid advisory model. That means the integration of robo-advice with traditional advice. This is at a time that a new group of investors – Generation X and Generation Y – come to account for most of the investable assets in the world. Success will come from delivering those investors the user experience, the insights and the functionality that they expect. This is the challenge that we are working with our financial institution clients to master.

Financial IT: What is unique about Dorsum and how it helps to stand out among its competitors?

Imre Rokob: Dorsum provides cutting edge cross-platform front-to-mid & mid-end software and mobile applications for wealth management and private banking clients. We have an experienced project team, with team members working at Dorsum almost since the beginning, gaining a lot of experience in multinational and complex projects. Furthermore, we offer the fastest and the easiest way in any core system integration and we use intelligent investment algorithms in our software solutions.

Financial IT: Could you please tell us about what will be Dorsum showcasing at Money20/20 Europe 2019?

Imre Rokob: We will showcase our newest solution My Wealth, a Wealth Management mobile app which serves the needs of the “new type” of investors. My Wealth is a unique app because it grants a hybrid advisory model and provides the best possible UX to the clients. It has integrated wealth management and trading functions and it has a simple, easy to understand, client-oriented wealth reporting system. It's Easy Invest function brings the complicated world of investments closer to everyone.. In addition to our software, we also offer an integrated service package to help develop a so-called wealth management ecosystem, where our customers are not only see us software vendors, but as strategic partners.

Financial IT: What are the major plans you have for Dorsum in 2019 and beyond?

Imre Rokob: We will be helping existing and potential clients to better understand key topics such as Artificial Intelligence (AI) and the second Payments Services Directive (PSD2), so that they can use our solutions to address issues and challenges that arise.



Imre Rokob

Imre Rokob is the Director of Business Development of Dorsum, responsible for the company's expansion to new international markets. He is an experienced PMP certified project leader with a strong IT and financial services background. He managed several software implementation projects in Central and Eastern Europe and has been the Project Director of the company for 10 years. Leveraging his broad experience in brokerage, asset management, wealth management and integration of banking systems, he has started to supervise product development projects for next generation tablet/smartphone trading and private banking applications.

INCLUSIVE BUSINESS BANKING IS NOT CLOSE ENOUGH FOR SMEs

Financial exclusion is an increasing concern for businesses. Companies of all sizes, but especially the smaller, younger firms, can be held back from meeting their full potential by difficulties with payments and cashflow. Transfers can be too slow and expensive, and without access to additional funds many SMEs struggle and potentially fail. Traditional banks are unable to provide flexible, fast and low-cost solutions, which leaves many SMEs financially excluded.

Banking Circle has built solutions to help businesses of all sizes compete and prosper. The suite of innovative Banking Circle solutions is increasing financial inclusion by providing previously excluded businesses with access to essential lending, banking accounts and cross border payments. We, therefore, recently commissioned Magna Carta Communications to carry out in-depth independent research to give us a unique insight into what is causing financial exclusion for SMEs – and the opportunities that exist for the financial services sector to improve financial inclusion.

The current landscape

There are more than 24 million SMEs in Europe. They make up over 99% of all the region's businesses, and account for two thirds of all employment. They contribute more than half of all business turnover and generate more than half of all value added in the non-financial business sector - worth €4,030 billion in 2016. These businesses clearly represent a significant opportunity, yet many find themselves financially excluded.

Some lenders are ahead of the curve and already providing dedicated solutions to better-serve companies where traditional

banks have been unable to help. For example, PayPal recently announced that it has provided £1 billion of finance to over 37,000 small businesses in the UK since it launched PayPal Working Capital in 2014¹.

However, it seems that fear of the unknown could be holding back SMEs from capitalising on the new solutions coming onto the market. It was recently reported that 51% of SMEs would still approach a traditional bank in the first instance, if they needed additional funding². The figure has, in fact increased since the previous survey a year earlier when 45% said they would approach a bank first.

And a recent Banking Circle survey of more than 500 SMEs revealed that without access to additional funding, 24.6% would have to cut employee numbers and 13.3% believe the business would fail. Therefore, this loyalty to traditional banks - despite SMEs confirming their lack of satisfaction with the service delivered and costs incurred - could cause small businesses to fail.

But there is light at the end of the tunnel. The Altifi survey, which involved 2,000 SMEs, also showed an annual increase in the number of SMEs considering using an alternative lender – up to 35% in 2019, from 30% in 2018.

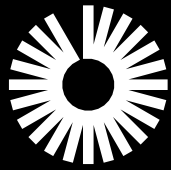
Barriers to better provision

There is a growing commitment to improving access to commercial banking, transaction services and lending for SMEs across Europe. But the multitude of issues at play means there is no one-provider-fits-all solution.

With Europe's SMEs covering every industry, with varying business models, distribution and ambitions, no two firms are

¹ <https://www.paypal.com/stories/uk/paypal-backs-uk-small-businesses-with-1-billion-of-cash-advances>

² <http://www.altifi.com/article/5204>



BANKING CIRCLE

Anders la Cour,
Co-Founder and Chief Executive Officer,
Banking Circle

Anders la Cour is a hands-on leader driving innovation to facilitate more inclusive, efficient and cost-effective banking, lending, payments and FX. He was also instrumental in arranging the \$300 million acquisition of Banking Circle by EQT VIII and EQT Ventures in 2018.



alike. This creates a barrier to providing effective and viable financial solutions at scale – neither existing corporate nor retail-focused offerings are suitable, so SMEs are left out in the cold.

There are plenty of ambitious, but still underserved, businesses with specific needs that could be met by an open, joined-up ecosystem. There are also plenty of potential providers of innovative ‘point’ solutions. But there remains a lack of connection between the two, apart from individual, often ad hoc series of collaborations. The bigger picture of a connected ecosystem – a circle of trust – is often obscured by a virtual tidal wave of statistics, audits and promotions.

The reality is that small businesses have specific requirements. Consumer products that try to attract SMEs, are often not agile enough and have little knowledge of small businesses. And the solutions developed for corporates are often too complicated for SMEs.

Making changes together

Without access to suitable solutions, SMEs find themselves facing high prices and other barriers to entry which are stunting growth and limiting the appeal of SMEs to prospective lenders – it is a vicious circle of self-reinforcing inaccessibility.

The current offering, or lack thereof, is perpetuating the difficulties for SMEs and in turn their higher-risk status from the point of view of the banks. To transform vicious circles into virtuous circles – of provision, availability and use – will require a more collaborative and creative approach, to build a mutually

supportive ecosystem in which SMEs can thrive and improve their contribution to the economy.

SMEs with access to suitable financial solutions are also better-placed to increase internationalisation and exports. This helps to support the diversification and resilience of the wider economy which in turn improves social integration and community cohesion. The significance of financial inclusion should not be underestimated.

The Enterprise Europe Network recently reported that 65% of small businesses expect to increase their turnover and 85% expect to create or preserve jobs in the next year. However, these ambitious companies need financial services providers equally committed to innovation and growth. Despite the EU recognising the importance of financial inclusion and bringing in policies and programmes to help deliver better access to SME finance, many SMEs are yet to reap the benefits.

The industry is at an inflection point. To move forward, I believe all ecosystem participants must continue the conversation and work together, to build collaborative models and solutions that can fit this diverse and disparate market. If they can, it will help build a larger marketplace from which providers old and new can benefit. We have seen evidence that there are significant gains to be made by all participants. But rather than relying on top-down directives from state institutions, this needs to be led by forward-thinking participants, who can find and build accessible and inclusive solutions from the bottom up.

The full report, Financial Inclusion for Europe’s SMEs: Building a circle of trust, will be published at Money20/20 Europe. Click here to register for a copy available from 3rd June 2019.

⁵ https://enterprise-europe-bw.de/fileadmin/user_upload/Baden-Wuerttemberg/Seiten/Publikationen/EEN_Report_SME_growth_forecast.PDF



WHAT ARE THE KEY TRENDS DRIVING PAYMENTS ACROSS EUROPE?

Consumer demand is rapidly evolving in the European payments landscape, with new innovations quickly emerging and regulations endeavoring to keep pace with the transformation. This is driving change in the way payment companies, merchants and banks operate.

The payments landscape across Europe is far more fragmented than many people realise but there are still some general trends to be observed. Driving the constant evolution of payments are huge external factors such as, the growth of eCommerce, online marketplaces and consumer behaviour becoming more digital. This is made clear by the fact that the volume of online purchases is still rapidly increasing.

This article will discuss the key trends across Europe, as well as shining the spotlight on key innovations that are gaining in popularity across the region.

The payment landscape

Consumers, across Europe, are favouring non-cash payment methods, such as debit and credit cards. These have overtaken cash payments, with the use of cash at the point-of-sale (POS) falling from 52% to 42% in 2017¹, as a result.

Omnichannel strategies are now a must for merchants operating in Europe, as eCommerce has grown steadily across the

continent over the past decade, a trend that is expected to continue. Europe's B2C eCommerce value was €602 billion euros in 2018, up from €530 billion the year before². Western Europe (including the likes of France, Spain, Germany and the UK) is still maintaining the greatest eCommerce market share across the continent, with 53.19%, while Eastern Europe has the smallest at 6.17%². The UK maintains its place at the top of the European eCommerce market chart but others are catching up across Northern and Western Europe, with companies such as Denmark and Germany enjoying similar levels of success.

eWallets

It is essential businesses do not forget Europe is highly diverse and fragmented when it comes to payments. Payment methods vary greatly across EMEA. Out of the countries in the region, Finland and Germany are expected to experience strongest growth in payments revenue up to 2021 with 31% of eCommerce in Germany being fueled by online banking solutions and eWallets³.

Europe is currently experiencing a fierce battle for eWallets and mobile payments. Global players such as Apple and Samsung are challenging traditional online payments systems (like PayPal), especially in the UK. Local initiatives have recently led to new

competition, for example, Lyf Pay in France, which is a collaboration between four banks and three merchants. Lyf Pay incorporates mobile payments, loyalty cards, coupons and online offers, as well as friends and family payments and charitable donations. In other markets, local alternatives still dominate, such as iDEAL an e-commerce payment system in the Netherlands.

While the growth of eWallets is a global trend, their rise in Europe is particularly strong. Consumers are adopting the technology to make payments online. This is true for eCommerce markets across the continent, regardless of whether they are more mature or less developed. In Italy, for example, just less than one in three online purchases are now made using an eWallet⁴.

Marketplaces

Amazon is the most prominent online marketplace across Europe's mature eCommerce market. Yet all are vital platforms for small retailers to compete in the online space, as long as their chosen portal can cater to an international customer base with localisation options and payment methods for each area. Germany's eCommerce landscape differs from the majority of Europe, with far more marketplaces than average – 39, followed by France with 24 and Italy with 14⁵.

¹ A McKinsey & Company, Global Payments 2017: Amid rapid change, an upward trajectory

² eCommerce Europe, European eCommerce Report 2017

³ The Paypers, Payment Methods Report 2017

⁴ Imrg: How will the European payments landscape change in 2019?

Gertjan Dewaele,
Head of Innovations at
Ingenico ePayments

Gertjan Dewaele is leading the Innovation & Airline & Travel product teams within Ingenico ePayments. He has several years of experience in e-commerce, in different roles at Ingenico and is passionate about new trends in payments, technology innovation and online consumer experience. Prior to that, Gertjan worked in strategy consulting at the Boston Consulting Group and he holds a Master's in Computer Science Engineering from Ghent University.

Ingenico ePayments is the online and mobile commerce division of Ingenico Group. With its global capabilities and expertise, Ingenico helps merchants optimize their business and grow into new markets around the world.



Social selling

The lines between social media platforms and marketplaces are blurring, but one truth remains, social commerce is growing across the region. For example, Facebook's consumer-to-consumer online marketplace, is operating in 17 countries across Europe⁵. Its uptake across the continent has been slow and the majority of retailers are not fully prepared for social commerce, however, there are early signs of consumer interest. For example, 45% of consumers in France aged 18 to 35 say they would like to make purchases directly on social media⁵.

What's more, chatbots are increasingly being adopted on social platforms. Businesses and customers are both reaping the benefits of this technology as it is helping them navigate platforms and resolve issues by offering quick answers and solutions.

What has been and what will be the impact of EU regulations on payments?

PSD2

Technological advancements will improve the experience of online and mobile payments, while the implementation of

PSD2 will lead to greater security and convenience. It will enforce more security via strong customer authentication (SCA) and a better user experience during the authentication process. Further, the implementation of Open Banking and similar regulatory changes will also make it easier for merchants to initiate payments online and via mobile. As a result of these comprehensive changes, customers will enjoy more choice in payments, as well as deeper integration of eCommerce into their lifestyles.

GDPR

Trends show a huge increase in data breaches and research shows that most companies have work to do in order to improve and enhance their cybersecurity practices. Companies should see GDPR as a sign of what the future holds and take data protection (and a robust approach to data management) seriously.

Data protection principles must be embedded throughout entire organisations and, as GDPR states, 'privacy by design' is a must. Regardless of a company's geographic location and its role in any payment chain, all organisations should embed GDPR principles within their day-to-day working.

Ensuring you are operating successfully

Europe is more mature compared to other regions when it comes to payments and will see steady growth of CAGR by 6.5%⁷. However, it is still not as advanced as Asia, for example, which is set to grow by a much bigger margin of 28.6%⁶. There are, however, significant shifts that can be seized to promote further progress.

Though it is safe to say, consumers are increasingly moving towards digital and cashless payment methods, while embracing eCommerce, it is important to consider the variation in consumer demand across the continent to ensure this advancement. Businesses must also be aware of this if they are to successfully compete in the market. Therefore, it is important for companies to partner with payment service providers that understand the region, especially as we see the emergence of new technologies such as social commerce and eWallets, along with the ongoing implementation of regulations such as PSD2 and GDPR.

- You can find out more about the evolution of payments across Europe in our latest report at: https://www2.ingenico.group/four_corners_of_payments

⁵ EU Gateway, E-commerce in Europe

⁶ eMarketer, Millennials in France Look Ready for Social Commerce

⁷ Ingenico ePayments: Four Corners of Global Payments



DIGITAL CONSUMERS: BORN OR MADE?

'Born digital' refers to materials that originate in a digital form. It also applies to people. It's now possible to be a fully-grown adult without having known a time before the internet. And similarly to have started a business exclusively in the post-internet era. What impact is this having on commerce, and how retailers, banks and payment providers interact and transact?

Once upon a time...

Digital natives never had to watch television at the time of transmission to see their favourite programmes. They never had to call a place, usually a home or office landline, to speak to a person. Or deal with stationery and stamps to write to someone. The first generation of digital natives is already here, which cannot but affect their expectations of suppliers and service.

However, it wasn't always this way. Almost every industry — retail, finance, entertainment and so on — seemed slower, simpler and more store-based before the internet. Consumers didn't know any different. They did not expect any better. The balance was tilted in favour of the suppliers. The same few firms dominated. New entry was modest. Innovation was

incremental. Products and services were static. Or at best similar to one another and to what they had always been.

Somewhere along the way, Jeff Bezos and others like him pioneered online shops. They thought that if they offered more choice online at lower prices, with the convenience of home delivery, it might catch on. They were right.

It wasn't merely the sales channel, but the proposition that caught on. Amazon rejected either/or thinking. What it offered was both low-priced and convenient. It was both fast and good quality. There were no trade-offs. Consumers did not have to settle for less. They expected more — and they bought more online.

Consumer-push or retailer-pull?

Twenty-three years after their first web shop selling books, Amazon is valued at more than \$950 billion. Global retail e-commerce sales stood at \$2.8 trillion in 2018 or 12 per cent of global retail sales, according to Statista.

Internet-enabled digitisation and disruption has created brand-new business models, such as search, apps and cloud computing. It has also turbo-charged

traditional models, such as classified advertising, affiliate marketing and marketplaces connecting buyers and sellers. So, is the digital consumer born or made? Is the move to digital commerce consumer-push or retailer-pull?

It's probably a combination of the two. Retailers shouldn't be looking to re-invent consumers. The first generation of digital natives, born and raised in the digital world, are the consumers of today. Whether they are digital natives by age or by attitude, such consumers are re-shaping the world in their own image.

At the same time, digital businesses are coming of age. They think differently as well as digitally. This mindset change is as powerful as any technology change, if not more so. Initially, digital was seen as a new way to automate old processes to cut costs. Or as a new channel to distribute old products. But the combination of consumer expectations, technology and regulation is driving new commerce.

What do customers really, really want?

Customers don't refer to themselves as 'e-commerce shoppers' or 'face-to-face shoppers'. To them it's just shopping.

Stefan Merz,
Chief Operating Officer,
PPRO Group



Commerce is moving from being channel-centric to being increasingly customer-centric. Enabled by intelligent systems and insight, customer-centric commerce personalises and customises the experience depending on, you've guessed it, the customer.

Done correctly, customisation is a win-win. Customers report higher satisfaction. Merchants report higher sales. Sometimes the experience will be entirely digital. Other times it will involve a digital element. Or be entirely analogue. Customers have different considerations and needs when they buy their morning coffee, pay their gas bill, order a take-away or purchase a second-hand car. Commerce is contextual. How and why people buy depends on so many factors. How and why they pay depends on a whole host more.

It seems counter-intuitive yet the more global and digital the commerce, the more local the payment. There are more local payment methods than ever before. These tend to follow consumers wherever and however they shop, at home or abroad, online or in-store.

Payment habits are strongly national. They have developed over time and are formed by various cultural, political, economic and technological factors. They differ between people within the same country, let alone between countries and regions. So, while commerce is about more than paying, offering a smooth payment experience is critical to a good customer experience.

PPRO's own research reveals that 67 per cent of UK consumers have abandoned an online retail site simply due to the payment process. Just over a fifth of these left because the process was too complicated, while a similar number didn't complete the purchase as the merchant didn't offer their preferred payment option.

It's not a case of digital versus analogue, e-commerce versus in-store. Customers really, really want an experience tailored to them. This frequently ends in being able to pay their way. Whether merchants are operating within their home market or expanding abroad, they have to localise payments to close sales.

Powering the digital future

While it's good manners as well as good business to localise payments, for merchants it's a catch-22. Greater customisation and simplification on the front-end creates greater complexity on the back-end. The right payments infrastructure is essential to allowing customers to pay anyone anytime, anyhow from any device or funding source.

Because digital consumers and merchants are born as well as made. Acquirers and payment service providers must help their merchants to increase reach and make customer journeys smoother. Payments play a central role in driving simpler, smarter and more customised experiences.

PPRO helps to make this part easier. When it comes to local payment methods across 175 countries, we are the payment professionals. We process, collect, reconcile, consolidate and pay out all on one contract and with one integration and platform.

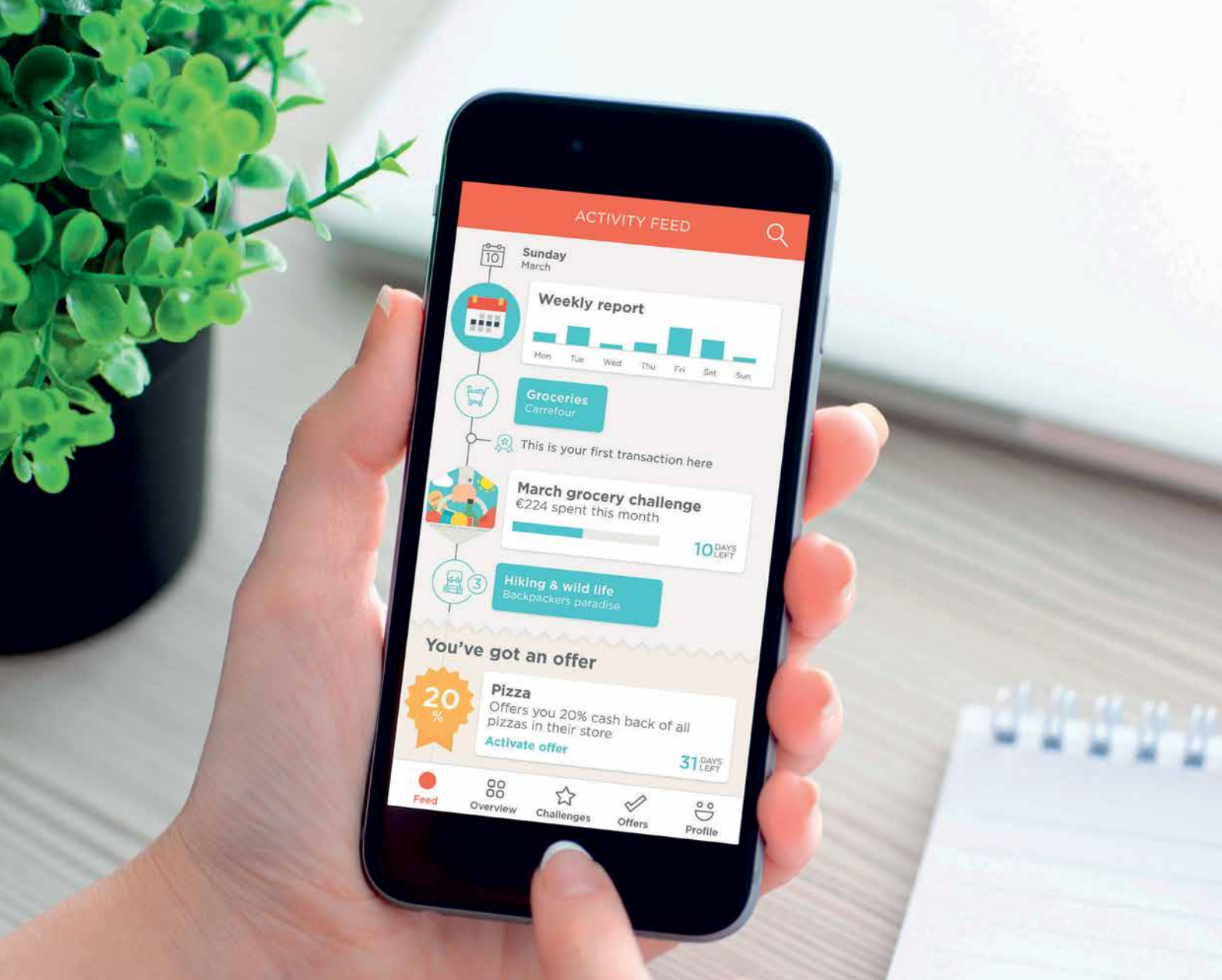
More payment methods mean more customers

People can only buy if you have the means to let them pay. For anyone running a cross-border e-commerce site, or expanding into a new market, that can be complicated. Payment methods often differ hugely from market to market. To not lose out on any potential customers, you need to know in advance what your new customers favourite local payment methods (LPMs) are.

The PPRO Payment Almanac lists and contextualises 450 payment methods, making it an invaluable resource for those in need of insight into the global payment landscape to inform global strategies and extend reach.

Visit www.ppro.com/almanac for your free 30-day trial!





Making Digital Banking **Personal**

We help banks build meaningful customer engagement and develop new revenue streams.

Want to learn more?
Visit meniga.com

 **meniga**

LOOK NORTH TO NAVIGATE eID SUCCESS

According to Arne Vidar Haug, Co-Founder of Signicat, digital identity has been solved. So why is most of Europe still getting it wrong? With federated eID firmly established in the Nordics, perhaps they're not looking in the right place.

With the increasing digitisation of lifestyles, proving “who we are” in the virtual world is a prerequisite to access services, buy and accept goods and initiate and authorise activities. For many organisations, including governments, financial services and telecoms providers, finding effective ways to confirm a customer’s identity seamlessly and without friction is crucial to success.

With so much to play for, establishing “federated” schemes that enable electronic identity (eID) portability across multiple organisations makes the most sense, particularly as businesses strive to cut costs, boost sales and enable better margins.

Europe struggling to gain traction

However, across Europe, efforts to create common hubs for sharing eID seem to be falling flat.

In Germany, only 18% of the population has activated the eID function on their national identity card. The UK has fared even worse: its GOV.UK Verify scheme is on life support, having reached a meagre 3% of the population in two years. Italy’s SPID initiative is also making slow headway with just over two million of its 60 million citizens signed-up. Meanwhile, Spain has invested heavily in an as yet unproven blockchain-based system.

Looking north, however, we see a different story. In the Nordic region, 70% of the population now have, and regularly use, federated eID across public and private sectors. What’s their secret—and how can they serve as a blueprint for the rest of Europe?

Banks take the lead in Scandi-success

Many factors have helped the performance of eID in the Nordics, but the most important of these has been collaboration and reuse of bank authentication credentials across public and private services. Public authorities didn’t go it alone, and instead were led by consortiums of banks that have pioneered adoption and achieved huge traction. This approach has

seen success for BankID in Norway (3.9 million users/74% penetration); BankID in Sweden (8 million users/78% penetration); NemID in Denmark (4.8 million users/85% penetration) and TUPAS in Finland (4.7 million users/87% penetration).

Banks have a huge advantage as they have already authenticated the majority of their country’s citizens for online banking. Linking credentials to the bank’s identity database (where personal identifiers are based on a thorough KYC process) makes bank issued eIDs equivalent to or stronger than a face-to-face ID check e.g. with a passport or physical ID card. It’s stronger because it isn’t based on ID verification alone, but also on the ongoing business record between bank and customer. Thanks to regulation and the simple fact that everyone needs a bank account, much of the heavy lifting has already been done. Why not use this?

Federated eID creates infrastructure for economic success

Appreciating their unique position, Nordic Banks chose to work together. Rather than ringfencing their investment in closed, competitive strategies, they joined forces

Arne Vidar Haug,
Chief Strategy Officer and Co-Founder, Signicat

Arne Vidar Haug is the Chief Strategy Officer and Co-Founder of Signicat, a verified digital identity solutions provider. Arne Vidar co-founded Signicat over 12 years ago, with the objective of helping businesses streamline identity verification processes by substituting physical ID-checks and manual document signing with electronic identification and signatures. As Chief Strategy Officer for Signicat, Arne Vidar is distilling the learnings over these twelve years into pragmatic strategies, technologies and processes that help organisations and individuals establish mutual trust in the online world. Over 200 financial services organisations across Europe and U.S., as well as governments and corporations work with Arne Vidar to implement effective digital identity solution strategies. As well as leading international growth for Signicat, Arne Vidar contributes to BankID, NemID, iDIN, MyBank, GSMA Mobile Connect and other digital identity schemes on behalf of Signicat.



to develop and implement a common platform that could be shared by all.

The result has been well-designed, well-used eID platforms that have formed the cornerstone of civic and social empowerment for citizens—providing secure access to government, health and social benefits and services. They are also delivering economic gains for banks' business customers by automating services and reducing administrative processes. In Norway, for instance, cutting mortgage paperwork using eID has generated annual savings of up to 10 million euros.

Many of the region's eID business customers report that they are happy to pay for these new eID services, as the benefits far outweigh associated costs. For instance, one rental service provider has seen 90% of its customers now sign-in online using eID—decreasing costs, boosting sales and generating stronger margins.

Nordic eID schemes have also become a valuable 'product' for banks, allowing many other services and organisations to accelerate, profit and thrive. For example, thanks to BankID, Swish in Sweden has been transformed from a mobile peer-to-peer payment system to the country's number two POS payment solution.

Learning points from the North

The Nordic eID road has not been smooth. It took Sweden, the first to initiate a bank-based federated eID system, 13 years for all major banks to get on board. However, Denmark needed only half this time to write its own success story, having learned what worked and what didn't from its close neighbours.

So what important takeaways do they offer the rest of Europe?

- Firstly, the best digital identity solutions are developed by strong, trusted partners who understand business and consumer needs, have the support of the government and who are able to offer users multiple applications for their eID.
- Secondly, a frictionless user experience is key. Registering for eID must be simple and preferably online—otherwise consumers simply won't sign-up. If it can be accessed any time, from any place, even better. In Sweden, Mobile BankID was the catalyst

that meant eID was part of 95% of the country's 2.5 billion transactions in 2017.

- Lastly, in order to build confidence and trust, systems must be secure, stable and 100% reliable. This requires a long-term commitment to investment, a strong focus and a future-oriented outlook from all parties involved.

As well as embracing these principles, banks must also park their fear of working with competitors and ally with other bank brands across traditional operational boundaries. By doing so, there's no reason why they can't successfully navigate eID to spread costs and build federated systems, recreating the same national adoption levels and commercial success enjoyed by their Nordic cousins.

Further insight and detailed country-by-country analysis is available in Signicat's latest industry report "Federated e-IDs as a value driver in the banking sector based on experience from Nordic markets".

SIGNICAT

Digital Identity On Demand



Chau Nguyen, Chairman, Ocular

THE COST OF KYC AND AML

Today every business needs to provide their banks the information needed to meet the regulations for Know Your Customer (KYC) and Anti-Money Laundering (AML). This has increased the cost of doing business with implementing systems to collect required information.

The banks have been fined \$26 billion for non-compliance during the last decade.

In Europe, 18 of the 20 biggest banks, including BNP Paribas, Société Générale, Santander, ING, Deutsche Bank, RBS, Barclay's and other big banks have all been fined. This demonstrates that no bank is immune to fines for offenses relating to money laundering since the financial crisis. This is an indication of how widespread money laundering has become.

The U.S. Department of Justice is the regulator that has fined banks the most — nearly \$14 billion. The New York Department of Financial Services comes in second, with \$3.6 billion. In fact, U.S. regulators have fined European banks nearly five times more than fines to U.S. banks.

Fines of top U.S. banks such as Bank of America, JPMC, Citibank and others have been in the billions of dollars. The cost of non-compliance is huge, and it is no wonder that banks are overly cautious with the companies and persons that they do

business with. This has opened a rapidly growing industry in KYC and AML solution providers. Ocular as one of the leading companies that provides businesses with the latest technology for KYC and AML.

What is KYC and AML?

KYC stands for Know Your Customer and recently is expanding to KYCC, Know Your Customers Customer. KYC is a regulatory and legal requirement for banks verify the identity of their customers. This is also used by businesses for similar processes.

AML is Anti-money Laundering, this is a set of procedures, laws or regulations designed to stop the movement of illegal money through a series of steps that make it appear that the money was earned legitimately. Every criminal activity drugs, kidnapping, extortion, bribery, etc. and every organization; terrorist cells, cartels, syndicates, hackers, etc. need to launder the money they have illegally gained. They do this cover their crimes and spend the money illegally earned without the authorities knowing, additionally they avoid paying taxes and other costs of doing business.

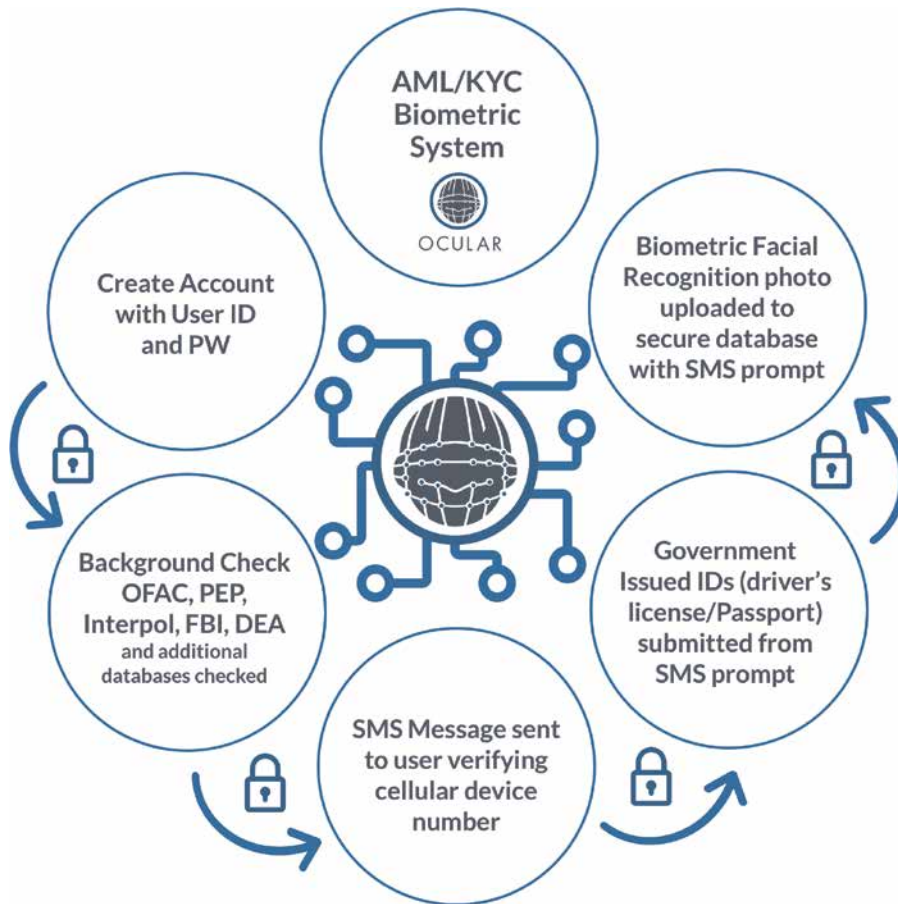
FATF (Financial Action Task Force on Money Laundering) is the central organization that calls upon all countries to bring their national systems into compliance with the FATF recommendations, and to effectively implement these measures.

The cost to the banks for a mistake are large, and companies are looking to reduce their financial crime risk. This has increased their need for partners, like Ocular, that can provide a fully automated KYC and AML screening solution. A partnership with Ocular provides access to the global databases covering sanctions, regulatory and enforcement watchlists.

How does KYC Help?

KYC is designed to prevent banks and companies from becoming involved with criminal activity. With Ocular, KYC is done by verifying documents obtained from reliable sources. This information may include the following; legal name, valid birth date, phone number, passport or a valid government issued ID, physical address (a utility bill or similar document), etc. The goal is to verify the identity and confirm that the person is correctly known. In addition to protecting for criminal activities, the KYC process also helps avoid identity theft and fraudulent account activities.

This gathering of information is what most companies do today. This information lets the company know that the customer they are working with is truly who they say they are. Most companies doing this level of identification will meet most standards and typically end their KYC/AML activities at this point. Now as a business you know that the customer you are dealing with is



the customer you know. What you do not know is has this customer been involved with any activities that would show up on any of the may watch lists. The danger for a company is that you may have a bad player in your customer base which puts your business at risk.

Protect Your Business!

Many business's do not realize the risks that not doing proper bank level watch list checking is. This is the protection that a partnership with Ocular can bring to your business. Ocular's solution integrates with your onboarding or registration process for your clients and will automatically check their names with the many global databases. It allows for instantly checking profiles of your clients on global and national sanctions lists including OFAC, AML, PEP, WMD, BSA, HMT, etc. and thousands of other governments, Interpol, United Nations, regulatory, law enforcement watchlists for financial and other crimes. A joint solution with Ocular

enables compliant-conscious businesses the use of a best-of-breed identity verification and AML screening solution. This can dramatically reduce the risks of a bad player in your client base, excessive manual reviews, reducing fraud and more importantly the scrutiny of your bank which could potentially damage this key business relationship.

The protection that Ocular provides is based on the usage of the latest technologies. Ocular is an Anti-Money Laundering (AML) compliance platform that provides instant verification of a customer's background (KYC). The platform leverages Blockchain technology to prevent any possibility of data tampering. Ocular uses name and personal data background checks that can be combined with state-of-the-art identity based proprietary facial and voice recognition. This safeguards against ID theft, false registrations, Sybil attacks and other attacks which compromise and circumvent compliance. Using advanced technologies such as Artificial Intelligence

(AI) and machine learning, Ocular can continuously monitor and upgrade its capabilities and defenses of cyber security.

Ocular provides a transparent method to verify and validate that prevents fraud and your expose to fraudulent activities. Ocular is a multi-purpose, customizable and configurable solutions that works for both FIAT and cryptocurrencies satisfying global bank level compliance requirements. This requires the automatic and instant checking of OFAC (Office of Foreign Assets Control), Interpol, PEP (Politically Exposed Persons), and other criminal databases to confirm an applicant's eligibility. A significant user convenience is the ability to enter their KYC/AML data only once into the Ocular Blockchain to be available for use with multiple platforms, websites, banks, merchants, financial institutions, etc.

We hope this information helps in understanding how important KYC/AML regulations are and how to protect your business. With Ocular as your partner, a positive user experience and more effective fraud prevention is possible, and that is a win for everyone (except the criminals). Importantly, strong KYC/AML procedures must be set up front. Best practices for using an automated identity process that safeguards customer information provides an accurate check and reduced manual review.

Whether you run a business, or you are a customer, KYC and AML matters. Everyone is affected by the cost of fraud and illegal activities. Business must do everything possible to keep improving these important functions. Companies are on the front lines, everything must be done to maximize the effectiveness of fighting financial crime.



BANKING ON SECURITY: FINANCIAL CRIME, POLITICS, AND THE AGE OF REPUTATION CRISIS

Irate customers, angry stockholders, doom and gloom reporters, even investigations by international law enforcement agencies – these are all just a few of the things a bank can expect if it gets caught up in a money-laundering scandal, where illicitly earned money is being used to fund criminal or even terrorist activity. But perhaps even worse than all those consequences is the damage to reputation – of the bank, and the bankers who presided over the train wreck that their venerable institution has turned into.

Just ask the folks at Danske Bank, perhaps the best-known – and most heart-wrenching – of the recent wave of financial scandals that have caught the attention of regulators. The details of the scandal, of course, are well-known. For nearly a decade, bad actors from former Soviet Union countries used the electronic banking facilities of Danske Bank's Estonian branch as their personal slush fund, moving illicitly and illegally-gained deposits through a bank that, until then, had had a sterling reputation for fiduciary discretion. The scandal cost the CEO his job, and will yet cost the bank billions in fines as regulators throughout Europe, and even the United States, begin examining the lesser secondary and tertiary scandals that are and will affect banks that had been doing business with Danske Bank – including Swedbank, and very possibly Deutsche Bank, American regulators believe.

Mistakes happen – that's the bottom line of the report Danske Bank issued about the scandal. "It was major deficiencies in controls and governance that made it possible to use Danske Bank's branch in Estonia for criminal activities such as money laundering," the bank's report said, blaming the scandal on "the lack of a proper culture for and focus on anti-money laundering at the Estonian branch," "inadequate governance in relation to compliance and risk," and poor management follow-up when alarms were sounded.

It's a serious indictment – but all of the issues laid out in the report can be, and will be fixed. However, the damage done to the reputation of institutions caught up in these scandals will be a lot harder to repair. The trust that was once there, the pride Danes had in their institution, one of the biggest and most influential in Europe, if not the world, is gone.

And the bank knows it. The Danish Financial Supervisory Authority (FSA) stressed this in its report on the scandal, saying that "the bank's Board of Directors had not identified and dealt with the risk and compliance-related deficiencies appropriately, which had created increased reputational risk for the bank." Management's "priorities and means of conduct have damaged the credibility and reputation of the bank. Considering the bank's

systemic significance and international presence, the reputation of the Danish sector of financial institutions may be damaged as well,” the report said.

While the reports discuss what can be done to prevent such scandals in the future, they don't discuss what Danske Bank has to do in order to restore its reputation – and that's because restoring a reputation is far more difficult than just making changes in processing, account verification, AML rules, etc. So how do you catch money launderers who are trying to hijack your account or processing system? It's not like they are announcing themselves, after all, the reason bad actors were able to fool Danske Bank's Estonian branch staff was because their transactions appeared perfectly legitimate. There are dozens of ways to mask where money comes from, and the AML staff at banks are not going to be able to keep up with all the new innovations in money-laundering.

Realizing this, five U.S. agencies – The Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Financial Crimes Enforcement Network (FinCEN), and the National Credit Union Administration – recently issued a joint statement calling on the financial industry to make use of private sector technology to help enforce AML rules. The agencies “realize that private sector innovation, including new ways of using existing tools and adopting new technologies, can help identify suspicious activity and combat money laundering and terrorist financing. Banks are encouraged to consider, evaluate, and where appropriate, responsibly implement innovative approaches in this area.”

What should those approaches look like? There are a plethora of solutions on the market. In addition, bankers need to be educated on advanced security and procedures, but at a minimum they need to include the following:

- **Wide Ranging:**

Money-launderers are able to ply their trade in part by hiding their transactions in the midst of ordinary ones. It's a fact, after all, that it took nearly a decade to track down the money-launderers who were using the Estonian branch of Danske Bank to move money. With billions of transactions a day, it's easy for suspicious transactions to get misplaced. The solution needs to be robust enough to handle that kind of load.

- **Automated:**

With billions of transactions to check, institutions obviously cannot rely on in-house teams to examine transactions. An automated examination system can check features of each transaction to ensure that they do not raise any flags that could indicate they were part of money-laundering activities. The automated system will flag all the transactions that need further investigation, bringing them to the attention of AML teams who can investigate them further.



Ron Teicher,
Founder and CEO of EverCompliant

Ron Teicher led EverCompliant from inception to become a leader in the field of merchant base fraud and transaction laundering detection. Today, EverCompliant serves some of the world's largest financial institutions. Prior to EverCompliant, Teicher led the compliance product initiatives at Watchfire (acquired by IBM). He is a member of the Israeli Bar Association, and is a frequent speaker at payment and fin-tech events. Ron holds a B.A. in Business and IT, and an L.L.B from IDC, Herziliya.

- **Intelligent:**

Money-launderers are always coming up with new methods of hiding their activities, so any system a bank installs must be intelligent enough to recognize those new methods as they are implemented. The system would be set to check data about a transaction such as the accounts the money is being transferred from or to, as well as the prior activity in that account, whether the amount being transferred appears appropriate for the account or customer, if it is based in a country under watch of international regulators, etc.

The agencies' point – and the lessons from the Danske scandal – is that banks need to do something to increase their AML vigilance. Failure to do so will end up costing banks dearly – in cash, and in reputation, a far more valuable commodity that is not so easily replaced.



EverCompliant
More Intelligence. Less Risk.

Mario Shiliashki,
CEO of Global Payments, PayU





THE ROLE OF FINTECH IN MAKING FRICTIONLESS CROSS-BORDER TRADE A REALITY

The last decade has seen the emergence of fintech and with it the monumental transformation of the global payments industry. In almost every area of finance, technology is transforming how things are done.

Convenience remains a major theme the world over, with consumers steering the payments industry with preferences that include a higher-degree of personalisation for a tailored experience, as well as connectivity, mobility and a global world view.

Seizing the cross-border opportunity

With consumer desire for a seamless, frictionless, global experience, cross-border trade arguably represents one of the biggest business opportunities available to merchants around the world.

Indeed, recent estimates have the cross-border market growing from \$401 billion in 2016 to \$994 billion in 2020, with nearly two-thirds of cross-border business coming from high growth markets including Asia and Latin America.

However, despite this significant opportunity, merchants are being held back by inflexible cross-border payment infrastructures and dated processes which make it hard for them to reach potential customers. The solution? Only by combining local market knowledge and new technology can these barriers be overcome and cross-border trade truly succeed.

The increasing consumer demand to buy internationally

The demand for cross-border trade is growing, fuelled in large part by the global rise in smartphones. Increasingly, tech-savvy consumers are demanding the one-click convenience they've grown used to. Unfortunately, cross-border trade has not yet caught up to this customer expectation, despite research finding that 56% of consumers shop far beyond their geographic boundaries.

The opportunity associated with local payment preferences

Historically, the payments ecosystem was burdened by complicated infrastructure and out-of-date processes. This remains one of the biggest challenges of cross-border e-commerce. The ultimate aim is to be able to offer frictionless payments experience to customers,

regardless of where they are located. In high-growth markets, this infrastructure problem is further exacerbated by the fact that alternative payment methods – which refer to payments made using something other than a credit or debit card like cash, coupons, bank transfers, loyalty cards, instalment products, etc. – still represent as much as two-thirds of all payments, and clearly preferred by consumers in these markets.

Platforms that bridge this interoperability and infrastructure gap amongst markets are critical in helping businesses reach a wider audience and seamlessly operate internationally.

The consumer credit conundrum

Coupled with historic payment ecosystems another issue faced by many cross-border merchants is a reliance on traditional methods of credit scoring which have proven ineffective for many consumers in emerging markets.

Understandably, many merchants from mature markets are hesitant to lower their risk threshold by relying on non-traditional payment verification models – creating an environment where it is incredibly difficult for businesses and customers to connect with each other.

Fortunately, another consequence of the rise in smartphones is that it brings with it a corresponding rise in data about a customer's spending and earning habits. As the volume of data increases, new techniques are being introduced to build credit profiles and more accurately understand an individual's credit rating. AI and machine learning are being incorporated into credit models, enabling underwriting which uses thousands of variables changing in real time.

The development of these new techniques will unlock credit and financial services for the underserved in these high-growth markets. According to some research, these advancements will aid the financial reach of over 1.6 billion new retail customers in emerging markets and will increase the volume of loans for individuals and business owners by \$2.1 trillion.

As fintech collectively harnesses the technology necessary for global financial inclusion, the attractiveness of high growth markets will only increase.

At the heart of this evolution is the focus on local market knowledge, local presence, evolving consumer preferences and ever-expanding merchant ambitions. This can further accelerate the growth of cross-border trade and ultimately change the lives of millions.

ULTIMATE INTELLIGENCE – AUGMENTING THE CHEMISTRY BETWEEN PEOPLE, TECHNOLOGY AND CULTURE



Shawn Rogers,
Senior Director of Analytic Strategy,
TIBCO

Shawn Rogers is an internationally recognised strategist, thought leader, speaker, and author specialising in analytics, business intelligence, Big Data, Cloud, IoT and social media technologies. He has founded and sold two Internet/media start-ups, and was formerly VP of Research at Enterprise Management Associates. He is presently the Senior Director of Analytic Strategy for TIBCO Software.

If Artificial Intelligence (AI) really was about replacing people, who would be the first victims? Surely those who endlessly repeat the same actions, with diminishing returns. However, machines are simply not set to replace the invaluable humans currently employed in financial services.

AI and Augmented Reality are not about putting these people out of work, their real purpose is to inspire human originality, by taking over the mindless repetitive work often found in the finance sector – and doing it a lot more efficiently too. This gives us time to inject intelligence into the tasks that we do, to re-examine how we can make a more powerful impact, and to innovate.

On the matter of innovation, a recent industry study explored the topic and focused on four terms – Experts, Experimenters, Conservatives and Beginners – that can be used to define an organisation's digital transformation maturity. Describing the first two groups in the hierarchy as the Digerati and the Fashionistas, the TIBCO CXO Innovation Survey defined these four groups by how they approach digital transformation, concluding that their ability to innovate and disrupt is defined by their progress, making the Digerati more likely to succeed.

A fundamental component of innovation is our readiness to change, and central to these four types of company is how they perceive that change will affect them. The Digerati and the Fashionistas have no fear of new ways of working, because they are in the vanguard and can see how it will work for them. They are self-driven and they feel in control. However, 'disruption' (the flipside of change) holds much greater challenges for those organisations lower down the hierarchy.

When considering disruption, it is widely understood that AI will ultimately

transform jobs, rather than replace the workforce. Interestingly, the study showed the most enthusiasm for innovation was expressed among leaders of change, such as Executive Management (where 19.76 per cent of people were identified as sponsors of innovation) and IT (17.43 per cent), but ultimately sponsorship is, and should be, spread throughout an organisation.

Likewise with augmented intelligence – which can be perceived as a more equal partnership of machine intelligence and humans – it is a partnership built on the three foundations of invention in a corporation: technology, people and culture. The successful amalgamation of all three is critically important for a successful innovation strategy.

Augmented intelligence works with the human qualities that AI alone cannot reproduce – and helps to build on them by offering assistance. Ironically this does not replace AI, but in combination, it can help AI be adopted quicker and more successfully.

According to CapGemini, only humans have the sophistication to identify errors and anomalies. Yes, AI systems can learn from their mistakes, but human supervision is still needed to ensure long-term success and widespread adoption.

Having said that, algorithm-inspired automation can power through bulk tasks and automatically identify exceptions. By doing the heavy lifting, AI gives those employed in financial services more time to apply their own form of intelligence and creativity. Let's use these smart people wisely, for the benefit of the industry and our customers. As augmented intelligence looks to catalyse a positive reaction between people, culture and technology, it's time to urge employees: don't be awkward, be augmented.



Send and receive money instantly
with **OlePay**, a secure and simple
payment solution.



www.olepay.com
info@olepay.com



**BANKING
CIRCLE**

**BANK ON INSTANT SETTLEMENT
BANK ON GROWTH**



Bank on us

Offer your merchants immediate cash advances against the receivables they're due. Our Instant Settlement service helps you develop new business while we bear the risk.

■ THE NETWORK FOR GLOBAL COMMERCE ■

bankingcircle.com

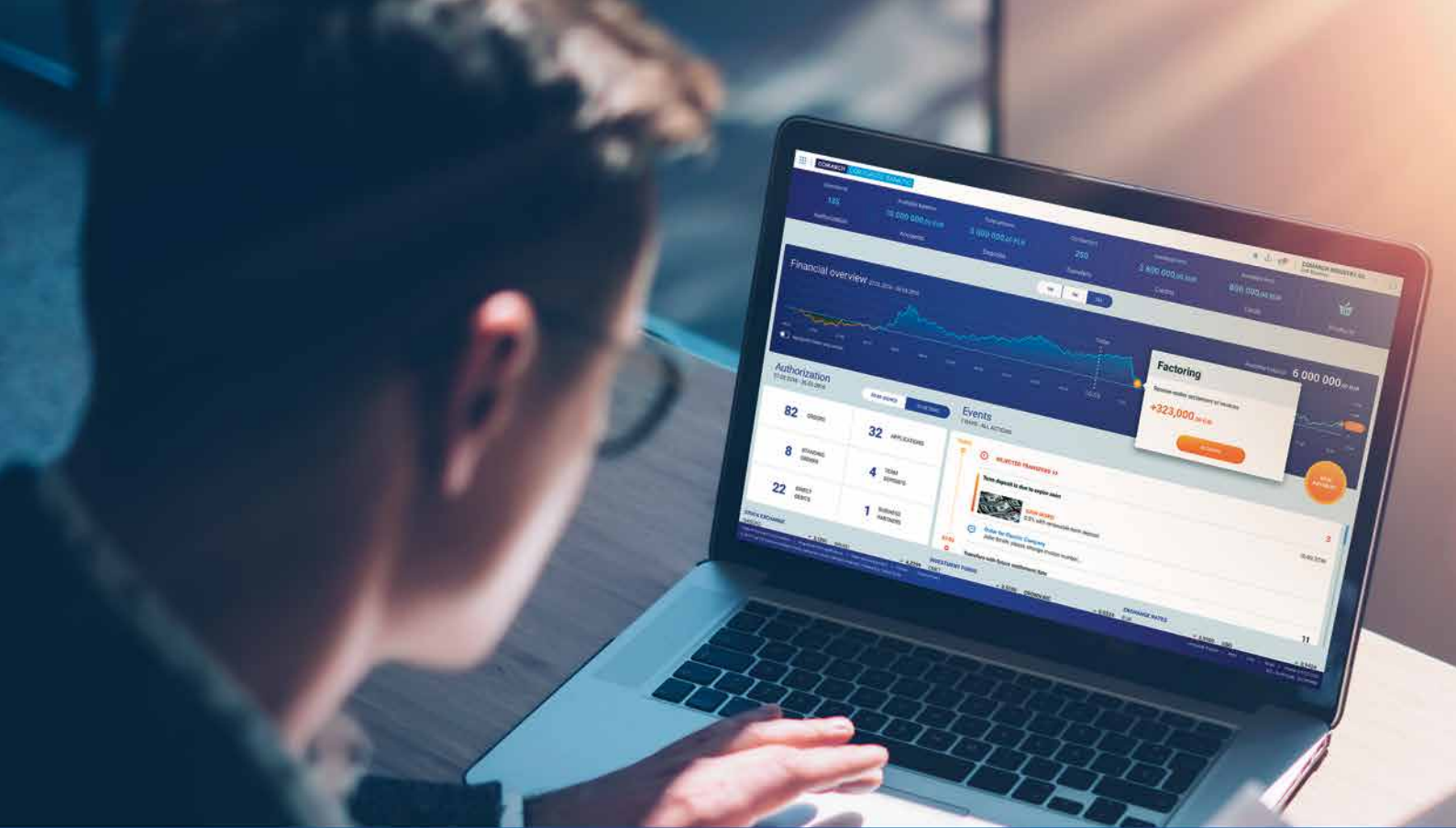
An aerial photograph of London, England, taken during the "blue hour" of sunset. The River Thames flows through the center of the frame, with the iconic Tower Bridge spanning across it. To the left, the sharp, glass-clad spire of The Shard rises prominently against the sky. The city's dense urban landscape is visible, with various buildings and structures illuminated by the warm, golden light of the setting sun. The sky transitions from a deep blue at the top to a soft orange near the horizon.

sibos

LONDON

23 - 26 Sep 2019

Register now!



Comarch **SME Banking**

Tedious procedures turned into a breeze



Quick time-to-market



Hassle-free integration across devices and channels



Straight-through processing of routine tasks



Focus on what really matters for your bank.
We'll get it to you in 6 months

COMARCH

Transform:Finance

Banking Cyber Security Forum

18th June 2019 - Docklands, London

**Boutique event,
exclusive to senior
banking executives
from global, digital
and challenger
banks.**



*"An absolute essential for modern day financial professionals."**

Andrew Fleming, Global FCR MI Senior Risk Reporting Manager, HSBC

*Describing previous Transform Finance event.

Join roundtable discussions and a top-flight agenda with:



Limited complimentary passes available - register now via

finance.transformindustries.com

"Bringing together financial institutions and vendors that are designing RegTech solutions to enable banks to implement better fincrime risk controls in a most effective and efficient manner."

Caroline Kennedy, Head of Financial Crime Control Operations - Corporate Banking, Santander

Proud to be partnered with:



Transform: Finance

Boutique conferences, exclusive to senior banking executives from global, digital and challenger banks.

"Events like these are an absolute essential for modern day financial professionals."

Andrew Fleming - Global FCR MI Senior Risk Reporting Manager - HSBC

Co-located on 12th September 2019 at the Marriott Hotel Frankfurt, Germany

Regulatory Reporting Innovation Forum

- Digital reporting innovation, including AI and robotic process automation (RPA)
- Improving data gathering, validation and processing
- SaaS solutions and reporting platforms

The Anti Money Laundering Forum

- Using AI to combat financial crime
- Know Your Customer and onboarding improvements
- Reducing false positives and transaction monitoring

"You'll learn, whatever level you are at in your organisation, it's always good to hear what peers are doing, and to hear what's developing as best market practice. Today has been very interactive and open, which has been really beneficial for me."

Aidan Paddick - Head of Compliance - ABN Amro Bank

Reduced early booking rates until 27th June 2019 - get yours now at

finance.transformindustries.com

Our Partners





FINOVATE

FALL
NEW YORK
SEPT 23-26

ASIA
HONG KONG
OCT 14-16

MIDDLEEAST
DUBAI
NOV 18-19

AFRICA
CAPE TOWN
DEC 5

**REAL
WORLD
SOLUTIONS
AND INSIGHTS
FROM FINTECH'S
CUTTING EDGE**

See the latest fintech innovations from around the world through unique, short-form, live demos.

Hear expert speakers share success stories and analyze the latest opportunities and challenges.

Connect with key innovators and influencers driving the future of financial and banking technology.

Only at Finovate.

SAVE 20%
ON YOUR REGISTRATION
WITH CODE
FKVFIT

Finovate.com



DIGITAL BANKING SOLUTIONS

LOAN FACTORY

The flagship productline of ApPello covers all phases of the lending process.

SMART BANKING SYSTEM

ApPello's Core Banking System is a perfect tool to handle effective clients, accounts, loans and deposit.

CASH OPTIMIZATION

AI solution for managing and optimizing physical cash in the branch and ATM network.

**ARE YOU INTERESTED?
REQUEST A DEMO:**

demo@appello.eu

