

# Financial Crime and Fraud Report 2023

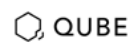
## Best Practices in Fraud and Risk Management



Endorsement partners:



Key media partners:



# Financial Crime and Fraud Report 2023

## Best Practices in Fraud and Risk Management

### Contact us

For inquiries on editorial opportunities please contact:

Email: [editor@thepayers.com](mailto:editor@thepayers.com)

To subscribe to our newsletters, click [here](#)

For general advertising information, contact:

Mihaela Mihaila

Email: [mihaela@thepayers.com](mailto:mihaela@thepayers.com)



RELEASE VERSION 2.0

JUNE 2023

COPYRIGHT © THE PAYPERS BV

DESIGN: MYRIAD DESIGN

ALL RIGHTS RESERVED

TEL: +31 20 893 4315

FAX: +31 20 658 0671

MAIL: [EDITOR@THEPAYPERS.COM](mailto:EDITOR@THEPAYPERS.COM)

# Foreword



**Mirela Ciobanu**

*Lead Editor – The Payers*



## When Did We Stop Being Courageous in Our Endeavours in Favour of Being Comfortable?

*Many people who work in Financial Crime Prevention began their careers with an ambition to ‘do good’. Heck, when we were kids who didn’t enjoy playing cops and robbers...and for some of us it even became a career. But somewhere along the way, the vast majority of us lost that sense of adventure and achievement that comes from catching the ‘baddies’. The job might have even become hard work and a thankless task. That’s no fun, right? And could we go as far as saying that because the current approach is so common, some of us might have given up trying to remedy the ineffectiveness?*

**Meagan Birch, MLRO & Head of Compliance**

**Step into the world of The Payers’ Financial Crime and Fraud Report, where the brightest minds gather to explore the ever-evolving landscape of financial crime and fraud detection. Our mission is to equip you with the latest trends, developments, and insights into prevention and management, empowering you to become an active force in creating a safer financial world. Join our community of proactive, forward-thinking individuals, and let’s work together to make a real difference. Get ready for an enlightening and invigorating journey.**

## What’s going on in the world (of payments) that makes this topic important now?

Did you know that financial crime has spiked during the recession? Fintrail points out that *customer fraud, scams, and organised crime activity have soared in the last 12 months*. And more interestingly, we’ve recently seen an alarming trend in consumer fraud too— that is fraud committed by consumers who don’t otherwise consider themselves cybercriminals. **According to Sift**, 16% of those surveyed by the company at the beginning of 2023 admitted to having participated in payment fraud or personally knowing someone who has. Another alarming phenomenon is *an increased money mule activity that supports money laundering*. Money mules are accounts used to receive illicit funds, whether it’s for fraudulent or money laundering purposes. Bad actors use various means to target money mules, such as instant payments/faster payments, internet banking, and transfers. Money mules are necessary for these types of fraud because fraudsters need a way to receive the funds, they are an essential vehicle for fraud.

At the other side of the spectrum, when it comes to fighting payment fraud, compliance, and the prevention of illicit funds movement in the financial system, the last twelve months have also seen *tremendous growth in the types of techs used* and the effort put in by large financial institutions to fight fraud and comply. The end of 2022 and the beginning of 2023 was the birth of ChatGPT which stirred a lot of controversy around what it can and can’t do for the financial world. As in all walks of life, *Artificial Intelligence (AI), machine learning (ML), and data analytics have emerged as powerful technologies, among the innovative regtech use cases, including risk assessment, regulatory change monitoring, communications security and compliance, Anti-Money Laundering (AML), Know Your Customer, and compliance reporting.* →

# Foreword

Still, as with many processes of financial systems (cross-border payments, checking the real identity of users, connecting different payment platforms, etc.), *one big issue that rises is the lack of harmonisation of systems and regulations across different jurisdictions* that puts a significant financial and operational burden on all market participants that are active across a specific region. For instance, diverging KYC requirements within the European Union creates fragmentation that comes with high costs and many lost opportunities, both for the bank, which cannot efficiently automate or standardise its controls and for the corporate, which is faced with additional and time-consuming KYC requirements, when it wants to expand its business activities across the EU or diversify its banking relationships internationally.

Hopefully, *the launch of a European Digital Identity Wallet (EUDI)* will change this situation. The EUDI Wallet can alleviate the complexity of onboarding customers or processing payments: being an electronic identification means with a high level of assurance, the EUDI Wallet can cut down the costs for KYC/AML, helping financial institutions fulfil specific regulatory requirements and build seamless online experiences.

Besides the EUDI initiative, what captured the public's attention in the European space are *the updates on EU's AMLD6 that are impacting FIs and crypto providers*. Companies operating in a transnational environment will need to take into consideration changes brought by the AMLD6 and pay close attention to the determination of the source of funds of their clients, as well as the dual criminality factor.

Most companies operating in the crypto sector have transnational activities. These activities will now need to be in line with FATF's Recommendations and Guidance, especially with Recommendation 15 (New Technologies), Recommendation 16 (Wire Transfers, also known as the 'Travel Rule'), and Interpretive Notes to them. Companies operating in the crypto sector will now need to have a proper licence (not just a registration for AML purposes) and collect originator and beneficiary information for all their digital assets – meaning they must know exactly where their assets are coming from and being sent to.

## Going beyond facts... let's put the cards on the table.

*Some of the facts and data we covered within the report have stirred a lot of discussion points.*

Take, for instance, enabling the so-called frictionless online journeys, which sometimes means removing screens and even reducing fraud design principles such as What You See Is What You Sign (WYSIWYS) on a separate trusted device, leading to poor security (in favour of great UX).

*Maybe we have gone too far by blindly parroting our digital teams' needs for fast onboarding, instant payments, and minimal user interaction while performing transactions.* To protect against fraud and economic crime, a solution could be applying *fraud regulations and enforcing in-journey accountability* (Han Sahin, ThreatFabric's CEO).

*AI, ML, and NLP are increasingly being used in banking fraud and anti-money laundering detection* to significantly improve banks' countermeasures and to ensure the integrity of the financial system. However, it will be essential for banks to invest in the necessary resources and expertise *to implement these technologies effectively and responsibly*. Several potential issues can arise *when implementing AI, ML, and NLP technologies*. One of the biggest challenges with AI, ML, and NLP is *the risk of biases and discrimination*. These technologies are only as good as the data they are trained on, and if that data is biased or incomplete, it can lead to inaccurate or unfair results. AI, ML, and NLP models *can be complex and difficult to understand*, which can make it hard to explain how decisions are being made. This lack of transparency can be a concern in industries like finance, where customers may want to know how decisions about their money are being made. →



# Foreword

Also, it's important to remember that AI, ML, and NLP are just tools, and they should not replace human judgment entirely. AI, ML, and NLP require access to large amounts of data, which can be a potential target for hackers or other bad actors. It's important to ensure that appropriate security measures are in place to protect sensitive data. There are of course other challenges concerning the use of these techs that are addressed in an extensive article within the report by Alan Morley and Fanny Ip from Huron.

Besides questioning the bias, lack of transparency, and AI accountability, Mark Haine, Founder, considrd.consulting also ponders over some *unintended consequences of the implementation of the EUDI*. Increasing the convenience of carrying and presenting identity information makes it much better for citizens, and the businesses they are dealing with, when things are going well. However, making it easier to share digital identity credentials *also makes it easier to over-share with a relying party that uses data in a way that the end-user has not agreed to or, much worse, easier to share digital identity information with a fraudster*. Another probably unintended consequence is that a *disproportionate burden falls upon people in lower socio-economic groups*. Despite the likely macro benefits of digital identity, the unresolved business model for using EUDI Wallets may have unintended consequences for some market participants, resulting in *some business entities losing out*. As such, we need to have further conversations on how we can address these (and other) consequences and *hope we get there in less than the 19 years it took payment wallets to overtake cards*.

*Bankers are also provoked to delve deeper into the topic of crypto.*

Colin Whitmore from NatWest Group provokes bankers to delve deeper into the topic of crypto by sharing best practices in preventing money laundering through cryptocurrency exchanges and custodian services. Cryptocurrencies are in the news daily, whether it is in headline-grabbing articles such as the sudden and dramatic failure of crypto firm FTX, or the use of cryptocurrencies in ransomware and other criminal activity. However, to claim that all cryptocurrency is used for criminal purposes would be a mistake. Not only does it disregard legitimate and legal investment, but it is a statement, often made without consideration of poorer regions of the world where the national Fiat currency is unstable, or access to banking services is expensive or limited. *So where does this leave FIs?* How should they approach cryptocurrencies, and importantly manage the risks? Relying on the Virtual Asset Service Providers (VASPs) themselves is not enough. Yes, some VASPs will have controls in place, with established KYC/CDD undertaken on their customers, and the ongoing monitoring of customer activity. *However, from a risk perspective, FIs need to understand and manage their risk, for themselves, especially where cryptocurrency is moved to and from Fiat currencies – the 'on/off ramps'*. Thankfully, there are several practical steps firms can take, which Colin explores within the report.

## There are humans behind fincrime (compliance)

Financial crime is a pervasive and insidious threat that requires a multi-faceted approach to combat. While technology plays an essential role in identifying and preventing fraudulent activities, we cannot forget the humans behind the fight against financial crime. The impact of financial crime is far-reaching, leaving many victims feeling despaired and abandoned. Regulators are often hesitant and concerned, unsure of how to effectively regulate emerging technologies like crypto. Industry practitioners are frequently discouraged by the lack of skilled and motivated individuals working in compliance and strive to see compliance as more than just a box-ticking activity.

However, there are also those enthusiastic and proactive fincrime fighters who are dedicated to learning and collaborating with their peers to spread the message and combat financial crime. We must recognise and empower the human element in this fight against financial crime to create a more effective and efficient system. →

# Foreword

## The power of storytelling

Working on the **Financial Crime and Fraud Report** enabled me to feel the creativity and humanity springing from the Fincrime Fighters contributing to this report. Some of the electrifying stories and metaphors I learned about include the **video of the turtle** with a straw stuck in its nose that galvanised the compassion of millions of people worldwide, and before we knew it, plastic straws became so unacceptable that we now have several alternatives which won't hurt turtles anymore. *In the turtle example, people – just like you and I, got active in creating new solutions. We harnessed a collective will and challenged big corporations to see the unintended yet harmful impact of their products and take our demand for change seriously. We would all benefit if we led a similar charge across Financial Crime Compliance (FCC).* **Meagan Birch, MLRO & Head of Compliance**

Compliance. The final tick box before a new product, service, or announcement goes live. Right? For a long time, this has been the case, but this approach of bringing compliance on board at the end of the process has stunted innovation. *An inexperienced baker would be foolish to glance briefly at a list of ingredients and attempt to bake a cake without following a recipe step-by-step. In the same way, those who are not experts in compliance should rely on the experienced compliance officer during product development to ensure the end product is compliant and ready for launch – like the best Mary Berry Victoria sponge.* **Mitch Trehan, UK Head of Compliance and MLRO at Banking Circle**

Putting the wheels on the AML suitcase – there are lots of wonderful, smart, enthusiastic, and talented young people in this industry. They have a very important role to play in the development of AML. Here's the context: *many years ago, when I was but a small boy, my dad would often carry two big suitcases when we went on holiday. Upon arriving at our destination, dad would be a little fatigued, sometimes irritable, and commonly sweaty. Why so? You ask. Well, it was because he carried the suitcases, as back then suitcases had no wheels. Imagine, if you will, the lunacy of suitcases without wheels. It references the simplicity of some wonderful solutions and innovations. Back to 2023 and the modern-day world of AML, it's not working, it is all too often, ineffective, and inefficient. Thus, it is the role of these smart young people to put the wheels on the AML suitcase and I am looking forward to seeing it in action, one day.* **Martin Woods, Cashplus and Global Compliance Institute (GCI) Chair**

Industry practitioners such as Meagan Birch, Dawn Fisher, Ray Blake, Dr. Ruth Wandhöfer, and Dr. Mario Menz have even a collective joke/metaphor for money laundering. *They were joking about cake and half-eaten hash browns as an illustration of our Financial Crime Compliance programmes and controls. We joked that our Transaction Monitoring systems were like half-eaten hash-browns and not very nourishing, that our compliance programmes were rarely as welcome as a cake when shared in the office, and that the office caterers (MLRO) had just resigned because anything they served was never good enough. We laughed but it got us thinking, critically, about how we have ended up in such a mess in FCC. →*

# Foreword

## Instead of a conclusion

But maybe the powerful message that resonated and stuck with me was this one:

*It's time for our industry to choose: do we just keep following a vision that does not resonate with our goals or can we focus on what inspired our career choice and collectively identify and try new approaches to make a difference? Let's find the straws in our Financial Crime PREVENTION approaches and create new ways to be effective against the 'baddies' who rob us all of peaceful communities. Let's turn the tide against complacency and illicit financial flows.*

Again Meagan!

It has been a long, exciting, filled with learning and networking opportunities, and a worthy journey to make this report happen! I hope I stirred your curiosity to continue reading it.

I want to take this opportunity to thank all our contributors that joined forces and delivered such educational, insightful, and powerful content. These are Victoria Sztanek – FINTRAIL, Esther Phillips and Rebecca Craig – Tenet Compliance & Litigation, Han Sahin – ThreatFabric, Alejandro Leal – KuppingerCole Analysts, Theresia Mallia – Kindred Group, Steve Pannifer – Consult Hyperion, Intesi Group, Mark Haine – considrd. consulting, Travis Jarae – Liminal, Maya Ogranovitch Scott – Ping Identity, Michael Ramsbacker – Trulioo, Thomas Egner – Euro Banking Association, Deborah Young and Alex Ford – The RegTech Association, Abhishek Chatterjee – Tookitaki, Ted Sausen – NICE Actimize, Mike Nathan – Feedzai, Sandy Lavorel – NetGuardians, Alan Morley and Fanny Ip – Huron, Colin Whitmore – NatWest Group, Ruben Menke, Robert Norvill, Christian Karsten, and Mitch Trehan – Banking Circle, Antonia Michail – Nuvei, Dan Aiello – IDVerse, an OCR Labs Company, Micheal Pettibone – Ekata, a Mastercard company, Jason Howard – Caf, Meagan Birch, Dawn Fisher, Ray Blake, Dr. Ruth Wandhöfer, and Dr. Mario Menz, Martin Woods – The Global Compliance Institute.

Of course, I would like to extend our gratitude to our esteemed collaborators (FinTech FinCrime Exchange, KuppingerCole, Consult Hyperion, Liminal) and media partners (QUBE Events) that will help us spread the message. If there is someone that I forgot to mention, do let me know, because in this fight against crime, all effort matters!

Enjoy your reading,

**Mirela**

# Table of Contents

3	<b>Foreword</b>
10	<b>Fraud in Payments and Fighting It with Technology</b>
11	<b>Financial Crime Risks in a Recession</b>   Victoria Sztanek, Research and Content Consultant, FINTRAIL
13	<b>APP Fraud: Pushing for Change</b>   Esther Phillips and Rebecca Craig, Litigators, Tenet Compliance & Litigation
15	<b>Navigating the Contradictions of Frictionless Online Journeys in an Age of Fraud Reimbursement; a ThreatFabric Perspective</b>   Han Sahin, Co-Founder and CEO, ThreatFabric
17	<b>Fraud Reduction and Authentication Enhancement for the Financial Services Industry</b>   Alejandro Leal, Research Analyst, KuppingerCole Analysts
19	<b>The Art of Balancing Risk and Customer Experience Expectations in Payments</b>   Theresia Mallia, Head of Payment Product, Kindred Group
21	<b>Unlocking the Power of Digital Identity</b>
22	<b>Using Digital Identity to Fight Financial Crime</b>   Steve Pannifer, Managing Director, Consult Hyperion
24	<b>The Role Played by eIDAS 2.0 in the Development of the European Digital Identity Wallet and Payment Wallets</b>   Viky Manaila, Trust Services Director, Intesi Group
26	<b>Potential Unintended Consequences of Implementing a Digital Identity Wallet</b>   Mark Haine, Founder, considrd.consulting
28	<b>Unlocking the Future of Digital Identity: the Key to Seamless Customer Experience and Business Growth</b>   Travis Jarae, Founder and CEO, Liminal
30	<b>Achieving Seamless UX, Robust Security, and Compliance in Digital Onboarding &amp; KYC</b>
31	<b>Know Your Customers: the Power of Digital Identity</b>   Maya Ogranovitch Scott, Solution Marketing Manager, Ping Identity
33	<b>The Power of Layered Identity Verification in Fighting Fraud</b>   Michael Ramsbacher, Chief Product Officer, Trulioo
35	<b>Generative AI in IDV: the Good, the Bad, and the Necessary</b>   Dan Aiello, CPO, IDVerse, an OCR Labs Company
37	<b>Trust in the Digital Age: Turning Consumer Trust into Revenue</b>   Micheal Pettibone, Senior Vice President, Identity Solutions, Ekata, a Mastercard Company
39	<b>Leveraging Optimal KYC and KYB Processes to Combat Fraud and Drive Revenue Growth for Financial Institutions</b>   Jason Howard, CEO, Caf
41	<b>The Benefits of Emerging Tech in Transaction Monitoring for FIs and Crypto Providers</b>
42	<b>Regulatory Landscape and Regtech Trends</b>
43	<b>Streamlining Low-risk Situations and Overcoming Other Roadblocks: the Journey to a Uniform European KYC Experience</b>   Thomas Egner, Secretary General, Euro Banking Association
45	<b>North American Regtech Trends</b>   Deborah Young, CEO, The RegTech Association and Alex Ford, President, North America, Encompass Corporation
47	<b>Embracing Community-Based Approaches and Innovation to Revolutionise the Fight Against Financial Crime</b>   Abhishek Chatterjee, Founder and CEO, Tookitaki



# Table of Contents

49	<b>Building Successful and Efficient AML Programs for Today's Business Environment</b>
50	<b>Transaction Monitoring in 2023: Changing the Status Quo</b>   Ted Sausen, AML SME, NICE Actimize
52	<b>Stopping Money Mules Using AI</b>   Mike Nathan, Global Head of Solutions Consulting, Feedzai
54	<b>Co-operate to Eliminate: a Community Approach to Beating Financial Crime</b>   Sandy Lavorel, Financial Crime Fighter, NetGuardians
56	<b>Integrating AI/ML/NLP for Financial Crime Compliance: Analysing Technical Complexities and Customised Implementations</b>   Alan Morley, Director, Anti Financial Crimes and BSA Advisory and Fanny Ip, Managing Director, Huron
58	<b>How to Strike the Perfect Balance Between Computer-Led and Human-Led Transaction Monitoring for Maximum Efficiency and Effectiveness</b>   Colin Whitmore, Head of TM Strategy, Innovation, and Design, NatWest Group
60	<b>From Rules to Models: Improving AML Decision-Making with Machine Learning</b>   Ruben Menke, Lead Data Scientist, Robert Norvill, Senior Data Scientist, and Christian Karsten, Head of Advanced Analytics, Banking Circle
63	<b>Key Considerations for Companies Entering the Crypto Market</b>
64	<b>Best Practices in Preventing Money Laundering through Cryptocurrency Exchanges and Custodian Services</b>   Colin Whitmore, Head of TM Strategy, Innovation, and Design, NatWest Group
66	<b>Updates on EU's AMLD6 that Are Impacting FIs and Crypto Providers</b>   Antonia Michail, AML Compliance Officer, Nuvei
69	<b>Join the Fight Against Illicit Financial Flows: Building Peaceful and Ethical Societies Worldwide</b>
70	<b>Courage, Cake, and A Half-Eaten Hashbrown: What Does This Have to Do with Turtles?</b>   Meagan Birch, MLRO & Head of Compliance; Dawn Fisher, Industry Practitioner, AML Trainer; Ray Blake, Director of Dark Money Files; Dr. Ruth Wandhöfer, Author, Speaker, Adviser & Coach; Dr. Mario Menz, Social Scientist, MLRO, and Head of Compliance
73	<b>Compliance to the Rescue</b>   Mitch Trehan, UK Head of Compliance and MLRO, Banking Circle
75	<b>The Importance of Working with Trained/Skilled People in the Fight Against Fincrim</b>   Martin Woods, Chair of the Global Compliance Institute
77	<b>Spotlight on Financial Crime and Fraud Fighters: the Leading Experts and Innovators in the Industry</b>
78	<b>Exploring Regtech, IDV Fundings &amp; Mergers – Insights into Current Trends and Future Projections</b>   Mirela Ciobanu, Lead Editor at The Paypers
63	<b>The Key Players in the Battle Against Financial Crime and Fraud</b>
83	<b>Who is Who in the Financial Crime and Fraud Fighting Space</b>
85	<b>Company Profiles</b>

# Fraud in Payments and Fighting It with Technology



*To deter fraud and survive in today's digital economy, financial organisations must be able to identify their customers from fraudsters or risk not only financial loss but also reputation and customer trust.*

Alejandro Leal, Research Analyst, KuppingerCole Analysts



**Victoria Sztanek** is a research and content consultant at FINTRAIL. A passionate anti-financial crime writer and researcher, she supports innovative anti-financial crime compliance teams and technology providers to develop effective approaches and solutions for preventing financial crime.

Victoria Sztanek ■ *Research and Content Consultant* ■ FINTRAIL

Economic conditions are likely to remain challenging around the world well into 2023. Against this backdrop, financial institutions should be aware of how economic downturns affect the financial crime landscape. As they often lead to more extreme behaviours, anti-financial crime teams are likely to see an uptick in criminal activity. We analyse three major risk areas for financial institutions.

### Customer fraud

Trying economic conditions mean that even 'ordinary' people with no history of financial crime can be lured into illegal activity out of desperation. Individuals pushed to a financial brink may commit acts of fraud such as making fake insurance claims, lending fraud (securing loans or credit cards using false information), or chargeback fraud (making a legitimate payment but then disputing it). They may also falsely claim they have been the victims of fraud and demand reimbursement from their bank - for instance alleging they have been tricked into sending money to a fraudster posing as a genuine payee (authorised push payment fraud).

In the workplace, acts such as forging timesheets or claiming false expenses, known as employee fraud, also tend to increase during a recession. This type of fraud can also involve more complex dealings like procurement fraud, where an employee pays a friend or family member to pretend they are a supplier or steal company data to sell to a competitor.

In a similar vein, individuals and companies may also commit tax evasion by inflating expenses or under-declaring profits to reduce the value of income tax or corporation tax they are required to pay. All these types of fraud rely on falsifying facts for economic gain.

### Scams

As people look for ways to supplement their income, they are also more susceptible to scams. Investment scams offer imaginary opportunities, promising high, guaranteed returns, and quick turnarounds. They can involve cryptocurrency, gold, stocks, foreign exchange, or even real estate. Taking advantage of cryptocurrency's elusive and volatile nature, crypto scammers impersonate businesses offering virtual coins or tokens, seeking investment, or giving faulty advice on fake cryptocurrencies. All these bogus investments typically involve a heightened sense of urgency and result in massive losses for victims.

Individuals looking for additional income may also become involved with multi-level marketing (MLM) scams. MLM promoters advertise an easy income stream, offering people a way to make money from selling products and gaining referral fees by recruiting new people into the scheme. In reality, selling the merchandise can be incredibly difficult, the schemes have hefty hidden fees, and promised commissions or referral payments are never made.

Romance scams involve social engineering tactics that falsify a romantic relationship with someone online. Once romantic feelings have been established and the scammer has gained the victim's trust, they will ask for money for emergencies such as fake medical bills. People are often more emotionally vulnerable when facing financial difficulties and may be seeking solace in companionship, leaving them more trusting and exposed than normal. Such people are the perfect victims of scammers, and financial institutions should be aware of the associated red flags. →

Also, on the theme of impersonation, impersonation scams are rife where fraudsters mimic genuine government bodies offering support such as energy and council tax rebates or encouraging people to apply for a 'cost-of-living payment'. Worryingly, **almost a quarter** of people in the UK feel uncomfortable saying no to a request for personal information from a stranger over a phone call. Coupled with the fact that these scammers can be very persuasive, impersonation scams pose a significant threat.

### Organised crime activity

Organised crime groups (OCGs) are smart opportunists during periods of economic recession. In addition to the money laundering risk, financial institutions should consider how vulnerable customers may become involved with criminality to alleviate financial hardship. Money muling is a crime that disproportionately affects the most vulnerable including students, young people, or unemployed people. It involves customers allowing criminals to move dirty money through their accounts to disguise the original source and flow of funds. Mules may make a commission per payment, or hand over their account to criminals for a fee. OCGs may also recruit individuals desperate for other sources of income for menial and not obviously criminal tasks. These may include translation services for human traffickers, couriers for drug traffickers, or 'running errands' that support the gangs' operations.

Difficult economic conditions make people more liable to take greater risks, increasing the number of potential human trafficking victims. During a recession, people may turn to riskier employment opportunities and can find themselves forced into sex work, paying traffickers to take them to more economically promising regions, or falling into debt bondage.

Finally, as cash and credit become more difficult to access, the risk of illegal loan sharking rises. This involves an unlicensed money lender offering loans at extremely high-interest rates. They often target individuals or families with low incomes and may use intimidation or the threat of physical violence to ensure repayment.

### What you should do

As economic hardship is foreseen to continue well into 2023, these financial crime risks will persist. Financial institutions should identify relevant red flags, be aware of changing risk profiles, and fortify their controls accordingly. Now is a good time to refresh risk assessments, do targeted assurance checks on anti-financial crime systems, and plan ahead to identify the need for increased resources, interim support, or more headcount as increased financial crime levels may arise.



[fintrail.com](https://fintrail.com)

**FINTRAIL** is a global anti-financial crime consultancy, working with leading banks, fintechs, and other regulated institutions. We help firms address the risks associated with the current cost-of-living crisis with custom-designed fraud monitoring programmes, risk assessments, systems testing, and training. For more information, please contact us at [contact@fintrail.com](mailto:contact@fintrail.com).

**com.**



# Tenet Compliance & Litigation

## APP Fraud: Pushing for Change



**Esther** is an experienced litigator with expertise across a wide breadth of commercial litigation matters ranging from straightforward breach of contract claims to complex cross-border litigation.

Esther Phillips ▪ *Litigator* ▪ Tenet Compliance & Litigation



**Rebecca** has 10 years of experience in trying cases and representing clients in high-stakes litigation and disputes, now specialising in fraud and financial crime compliance matters.

Rebecca Craig ▪ *Litigator* ▪ Tenet Compliance & Litigation

### Why does APP fraud remain a concern?

In our previous article in [January 2022](#), we discussed how APP (Authorised Push Payment) fraud occurs when someone is tricked into sending money to a fraudster posing as a genuine payee and what changes were on the horizon. In the UK, we saw the introduction of the Contingent Reimbursement Model ('CRM') Code which came into force in May 2019 and seeks to protect victims of fraud. The CRM Code is a voluntary scheme that sets standards and details when repayment should be made for those Payment Services Providers ('PSPs') who have signed up – the majority of high street banks are signatories. However, the CRM Code is not applied consistently by PSPs and there is a tendency to rely too heavily on the exceptions within the CRM Code to avoid repayment. Often victims of fraud can find themselves being challenged by banks stating the victim customer received an effective warning or is accused of gross negligence as to being careless with their security details, both of which were not the intention of the CRM Code.

### Proposals for change

The Payment Systems Regulator ('PSR') has identified that APP fraud continues to be a significant source of loss for consumers. In 2021, victims were defrauded of at least GBP 583 million as a result of APP scams. The PSR identified that there are three measures that they believe could help to reduce APP scam losses and

on 11 February 2021, they [published a consultation paper](#) detailing these measures.

These are:

1. Publication of fraud data by banks
2. Improvements in scam prevention
3. Mandatory reimbursement of victims

By introducing these measures, the PSR seeks to achieve improved outcomes for customers as they estimated that the overall level of reimbursement was less than 50% and this figure varies significantly depending on the PSP.

### Publication of fraud data by banks

The first of these measures is the publication of data on performance relating to APP fraud. The PSR confirmed, on 23 March 2023, that they had directed 14 of the UK's largest PSPs to collect and provide data on the proportion of victims of APP scams who do not get reimbursed and the rates of APP scams happening within the PSPs. The first report will be published in October 2023 and on a six-monthly basis thereafter. With this knowledge, customers will have greater transparency on which payment firms have not only the highest level of scams reported but also which payment firms have low levels of reimbursement. This will undoubtedly influence a customer's decision as to whom they choose to bank with. →

## Improvements in scam prevention

A crucial tool in scam prevention is the Confirmation of Payee ('CoP'). The service is designed to prevent payments by checking the name of the account holder with the account number and sort code. On 11 October 2022, the PSR announced plans to see 400 more financial firms provide CoP. There are currently 59 institutions offering this service and with greater reach, the number of APP scams will hopefully continue to fall.

## Mandatory reimbursement of victims

In the face of growing harm from APP fraud, the Treasury Committee called, in November 2019, for the CRM Code to be made mandatory. Following up on that recommendation, in February 2022, the Treasury Committee's *Economic Crime* report called for urgent legislation to make reimbursement mandatory. The Financial Services and Markets Bill currently making its way through Parliament will require the PSR to establish a system for mandatory reimbursement of APP fraud over the Faster Payments system. The Treasury Committee has recommended that the system should be fully implemented by the end of 2023. In response, in September 2022, a **second consultation was published** by the PSR indicating that there would be a mandatory requirement that all PSPs would be required to reimburse APP scam victims with only very limited exceptions and that this reimbursement should be as soon as possible, i.e., no more than 48 hours from the fraud being reported. There will of course be exceptions to this rule, such as where customers have acted with gross negligence. However, the PSR has indicated that this is a very high bar and will only apply in a small minority of cases. In addition to the above, the proposed changes include a minimum claim threshold of GBP 100 claim, a GBP 35 fixed excess fee, and a time limit of 13 months to present a claim. Furthermore, the costs of reimbursement will be allocated equally between sending and receiving PSPs, with a default 50:50 split. However, PSPs can use a dispute management process to adjust the allocation to better reflect the steps each PSP took to prevent the scam. The development of causing recipient PSPs to contribute to the compensation to victims is seen as a significant development.

## Implications for banks and PSPs

At present, should a customer be reimbursed as the victim of an APP scam, the majority of the payment is picked up by their own bank. In fact, PSPs on the receiving side of transactions now account for a negligible share of reimbursement (less than 5%).

This has the effect of the receiving bank having very little incentive to increase their fraud protection measures for incoming payments. It is often the case that those payment providers receiving the payment would have an easier job of identifying the fraud due to the nature of the account and its use.

Either way, the mandatory reimbursement requirements are likely to lead to significant new costs for banks and other PSPs. However, with the introduction of the mandatory publication of data running alongside these changes, it would be somewhat of an own goal for PSPs to resist the changes.

## Conclusion

PSPs need to ensure that they are taking appropriate steps to ensure that they are able to implement the proposed changes. There will need to be internal education in terms of when a customer should be reimbursed but also changes to policies and procedures to ensure both incoming and outgoing payments are flagged earlier, and the fraud prevented in the first instance.

From an outward-facing perspective, PSPs may wish to put more of an onus on the education of their customers to reduce exposure at the source. We are likely to see continuing pop-up warnings which evolve to ensure effective warnings about the risk for customers are just that, effective enough to cause customers to think twice before a transaction if they have any concerns.

The publication of fraud data will be very telling as it will be immediately obvious to consumers who have taken the time to invest and care for their customers and seek to protect them from fraud.



[tenetlaw.co.uk](https://www.tenetlaw.co.uk)

**Tenet Compliance & Litigation** is an award-winning boutique compliance and litigation law firm that helps organisations manage their financial crime regulatory obligations, investigate fraud, and provide advice on business disputes arising from business crime. Our expertise covers the spectrum of preventative action in the form of training and policy advice, through investigation and litigation advice. Our clients include banks, fintech financial services businesses, listed companies, not-for-profit organisations, and SMEs.

# ThreatFabric

## Navigating the Contradictions of Frictionless Online Journeys in an Age of Fraud Reimbursement; a ThreatFabric Perspective



**Han Sahin** is the CEO and Founder of ThreatFabric, and the previous owner of Securify (2012-2021). With more than 16 years of cyber fraud experience on both sides of the table, Sahin's vision is to empower banks and financial institutions to combat payment fraud using innovative fraud detection solutions.

Han Sahin ■ *Co-Founder and CEO* ■ ThreatFabric

### I. Introduction

#### A. The increasing focus on frictionless online journeys

In the past years, we have been asked by online payment teams to enable so-called frictionless online journeys. The implementation of this request means removing screens, adding additional consent steps, and even reducing fraud design principles such as What You See Is What You Sign (WYSIWYS) on a separate trusted device. After spending time in the UK with the PSR and anti-fraud community members, we have observed a lack of discussion on this controversial topic. However, we believe that attaining a balance is achievable through collaborative efforts, as this heightened focus on frictionless journeys is now not only affecting fraud and risk managers. It appears we as fraud protection vendors are now parroting an 'everything must be frictionless' strategy by enabling so-called frictionless fraud controls. By doing so, tipping the scale in favour of convenience versus security for customers. Even after consulting advisors, regulators believe it is acceptable to enable authentication controls that are weak by design to ensure an easy user experience as a top priority. PSD2 regulations have shown that SMS-based One Time Passwords or Second App Authenticators are considered a second Strong Customer Authentication (SCA) MFA-factor. However, there are many exploits in the wild (by malware and SIM swapping) introducing a false sense of security. It is in our best interest to question if we have gone too far by blindly parroting our digital teams' needs for fast onboarding, instant payments, and minimal user interaction while performing transactions. Is there even a way back when PSD3 dictates more consent on critical actions?

### II. The tension between convenience and security

#### A. Risks associated with frictionless experiences

Establishing permanent solutions to prevent online fraud is a challenging task. Complex fraud controls require accountability in an age of new reimbursement rules. Now in 2023, the fraud protection industry can solve very complex problems such as APP fraud where the victim is coached to execute a malicious payment. However, these new protection technologies require strong interaction with input fields, complex navigation, and even new consent screens to alert a victim that a fraudster could be coaching them to take critical actions. Banks and financial institutions, therefore, struggle with teaching users how to avoid fraud whilst delivering an enjoyable and seamless customer experience.

#### B. Customer consent and in-journey accountability

Fraud regulations for in-journey accountability consist of measures and policies defined to protect a customer's journey from various angles against fraud and economic crime. This approach seeks to determine which parties (banks, customers, third-party service providers) should be held accountable for security lapses that lead to fraud incidents during different steps of the customer's banking journey. A longer user journey may be necessary as it requires time to model the digital behaviour of a potential victim and fall back to normal payments (from instant payments) when there are strong fraud indicators present.

Although a customer journey with additional touchpoints may appear inconvenient and distracting from performing the task at hand, these measures ultimately serve to protect against fraud and unauthorised transactions. As the industry adapts to new →

reimbursement rules, complex fraud controls are necessary to maintain accountability and protect both institutions and customers.

*Will your customers feel more secure if they never have to show their key or prove their identity?*

### III. Key fraud controls and their impact on user experience

#### A. Ensuring Secure Experience (SX) in customer payment journeys

The future of online banking will consist of a rat race between which banks provide reimbursement based on proper authentication and fraud controls. Having a good Secure Experience (SX) serves as a strong USP for any payment team. It emphasises the protection of sensitive user information and the prevention of unauthorised transactions. This consists of robust authentication methods, encryption, real-time fraud monitoring, and adherence to industry standards and regulations. It effectively minimises the risk of fraud and data breaches through which payment teams can build trust with customers, differentiate from competitors, and encourage long-term loyalty.

#### B. Adding required in-journey steps

We advocate for interdepartmental discussions within organisations to address the inclusion of consent screens, the addition of steps between critical actions, and the necessity of requesting interaction with input fields. For example, fraud technology currently exists that can create supposed in-journey adaptive trust decisions.

Low risk-users that do not have fraud indicators can have certain steps removed in their online sessions (less friction, not frictionless), whereas high-risk users require more consent and interaction. Although these strategies are not widely adopted today, we still believe there is hope enforced by new regulations surrounding fraud such as APP fraud in the UK, which will require payment organisations to rethink their strategy moving forward. Ideally, this will result in a balanced world of less friction versus completely frictionless by parroting the requirements of payment departments dictated through fast onboarding numbers. The bigger underlying problem is working in strong silos, and the related organisational governance parroting important decisions that impact the ability to prove fraud.

### IV. Conclusion

#### A. Emphasising the importance of finding the right balance

In conclusion, fraud regulations and enforcing in-journey accountability are a step in the right direction to protect against fraud and economic crime. While frictionless payment methods are desirable, they need to be balanced with accountability to ensure a strong foundation before moving towards reimbursement. To achieve greater security, the industry should adopt stricter regulations when opening accounts and create accountability by introducing more friction in the journey flow, such as asking for consent and confirmation. Regulators should also consider implementing more stringent oversight and enforcement measures. Payment teams could benefit from creating fraud fusion centres that include equal shareholders to move away from silos. Ultimately, the industry needs to ensure that the feeling of security is prioritised and that the cost of fraud is reduced by implementing strong fraud regulations.

[Click here for the company profile](#)



[threatfabric.com](https://threatfabric.com)

**ThreatFabric** utilises web and mobile threat intelligence to offer advanced online fraud detection solutions for the financial industry. Their cutting-edge technologies, such as behavioural analytics, device fingerprinting, and adaptive fraud indicators provide businesses with real-time fraud prevention and detection to ensure safe online experiences.



# KuppingerCole Analysts

## Fraud Reduction and Authentication Enhancement for the Financial Services Industry



**Alejandro Leal** is specialised in digital transformation in the public and private sectors, managing a business in today's geopolitical context, and governance in artificial intelligence and cyberspace.

Alejandro Leal ■ *Research Analyst* ■ KuppingerCole Analysts

Fraud is one of the biggest concerns for businesses around the world. Fraud perpetrators are constantly looking for ways to obtain personal information such as email addresses, usernames, passwords, phone numbers, credit card numbers, and other financial details. Since the financial sector is one of the most targeted industries by cybercriminals, innovation tends to be a strong driver in this space. However, traditional authentication methods used by banks and other financial services organisations have proven to be fundamentally flawed in today's threat landscape.

To deter fraud and survive in today's digital economy, financial organisations must be able to identify their customers from fraudsters or risk not only financial loss but also reputation and customer trust. Unfortunately, credential-based attacks, phishing attacks, and account takeover fraud (ATO) cases have been on the rise in recent years, which have disrupted businesses and organisations already consumed by the COVID-19 pandemic and an uncertain geopolitical climate. To add fuel to the fire, the spike in fraud cases has coincided with the shift to remote and hybrid work and the deliberate targeting of remote workers.

Data breaches at financial institutions, their service providers, and credit bureaus, often involve the use of stolen credentials and compromised passwords. As a result, discussions around user experience (UX) and security are becoming increasingly popular in the authentication space. Due to changing business and security risks, as well as the availability of newer technologies, many organisations are seeking to adopt better methods of authentication that go beyond the traditional username and password. While the elimination of passwords has been a goal for a long time, it is finally starting to gain real traction in both workforce and consumer use cases.

By modernising their authentication methods and eliminating passwords, financial organisations can implement an approach that is scalable, secure, and user-friendly. For years, IT professionals have discussed the idea of removing passwords from the authentication flow. The problem with passwords is that they can easily be stolen, guessed, and compromised. Password resets can also be costly and time-consuming. Thus, relying on passwords for security has become increasingly risky and problematic for organisations in the financial industry.

With the rise of financial technology (fintech), which uses mobile devices and applications to facilitate financial services, many banks and financial institutions started to use fingerprints and other biometrics to enrol and authenticate their users. Initially, privacy and security were the primary concerns of organisations and individuals when it came to biometric authentication. While these concerns are still prevalent and justifiable, biometric authentication has gradually become increasingly accepted and even embraced by most users.

Biometrics is not a new concept or a new technology. Nevertheless, the rise of biometrics as a service has created a competitive, innovative, and dynamic market segment, thereby propelling the demand for passwordless technologies. The concept of passwordless authentication is already innovative in and of itself. The term passwordless authentication is used to describe a set of identity verification solutions that remove the password from all aspects of the authentication flow, and from the recovery process as well. If users lose or change devices, their accounts must remain accessible. To ensure users can securely regain access to their accounts without sacrificing user experience, a variety of trusted recovery options should be available. →

Some of the distinctive features of passwordless authentication solutions include the ability to support a wide range of authenticators, the use of biometric technology and public key cryptography, a consistent login experience across all devices, the introduction of a frictionless yet secure user experience, and support for legacy applications and services, among other things. Passwordless solutions are typically used alongside other authentication processes, such as multifactor authentication (MFA) or single sign-on (SSO), and are becoming more popular as an alternative to traditional username and password authentication.

Passwordless authentication solutions must provide customers of financial organisations with a smooth and frictionless user experience, but not at the expense of security. By continuously verifying whether or not each registered device meets the security requirements, passwordless authentication solutions validate and ensure that each device belongs to an authorised user. Some of the risk signals from the user and their device's security posture include device jailbroken/rooted check, device location and geofencing, the presence of a secure enclave, the presence of anti-malware, biometric authentication and firewall enablement, hard drive encryption status, and OS version, and more.

In addition, many passwordless solutions in the market provide cryptographically signed transaction confirmations that follow FIDO's 'What you see is what you sign' principle which is fully compliant with PSD2 Strong Customer Authentication. PSD2 is a new European regulatory requirement that aims to reduce fraud and make online and contactless offline payments more secure. In Europe, the collection of personal data by consumer IAM and authentication systems must adhere to a growing number of standards and privacy regulations. Financial organisations are also subject to Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations in various jurisdictions globally.

Passwordless authentication can be implemented across different industries wherever identification and authentication are required. The practicability of passwordless authentication depends on the use cases they intend to address. As a result, there is a great deal of variation in the deployment, usability, and interoperability of both different passwordless modalities and vendor implementations. A growing number of cybersecurity threats pose significant risks to banks and financial services organisations, resulting in millions of dollars in losses and stiff penalties resulting from regulatory non-compliance. Thankfully, the Passwordless Authentication market is growing rapidly. If implemented successfully, a passwordless authentication solution will not only increase security and drastically reduce fraud but also deliver a convenient and frictionless user experience.



[kuppingercole.com](https://www.kuppingercole.com)

**KuppingerCole Analysts** is an international and independent IT analyst organisation headquartered in Europe, with a presence worldwide. We specialise in the strategic management of digital identities, privileges, authentication, and access control as well as cybersecurity and business resilience.

# Kindred Group

## The Art of Balancing Risk and Customer Experience Expectations in Payments



**Theresia** is passionate about how payment innovation is transforming the ecommerce landscape. She has worked in ecommerce for over 15 years. Theresia has been involved in launching large ecommerce sites all over Europe, the Middle East, and Asia and she decided to move to iGaming six years ago to specialise in payments and improve payments products at Kindred Group.

Theresia Mallia ■ *Head of Payment Product* ■ Kindred Group

*During 2022, we saw PSD2 being rolled out in Europe; now, PSD3 is on the move. It is true that businesses and end-users can now benefit from improved protection with SCA and Open Banking. But I know there is so much more that can be done by the card and banking industry to go a step further. Especially around maximising the use of data that currently sits within the bank/ card schemes or card type payment options and cannot be maximised by merchants to avoid fraud/AML/third party deposits/underage and responsible issues/ gaming implications in some industries.*

**What are the implications of this:** *At the moment, merchants have no way to verify that the card belongs to a customer. 3DS helps to confirm the client has control of the device/card but does not prove if the client is using their own card. This means that the client's experience when using cards is not optimal, as in some industries they are still asked to provide documentation proving that the card belongs to them.*

### Verification of card ownership

For various wallets/bank payment solutions, it is possible to obtain customer information as part of the payment flow and match that with the customer's name to identify third-party deposits. This is not the case for cards and we believe it is quite an important gap in card payment services.

### So, what improved with PSD2?

When it comes to card deposits, a lot of merchants rely on the 3DS2/SCA part of PSD2. PSD2 allowed merchants to share their own customer's name as part of the card transaction, by sharing additional

customer details with card issuers (banks issuing the card), they will have the ability to check that the name is actually the card owner's name. However, we have no visibility if this check is being done, or which issuers conduct these checks.

### What else needs to happen?

The verification of ownership of the card is not currently included under PSD2.

We know that card issuers ultimately have visibility of the customer details. Therefore, in theory, there could be tools offered by card schemes that will allow merchants to verify that the card belongs to the customer (verify account ownership).

- **Option 1:** Card schemes can provide such 'customer match/no match' tools in collaboration with card issuers. Such products could help reduce fraud/money laundering risks through third-party deposits across various industries and should be implemented by card issuers.
- **Option 2:** Since customer details are shared as part of card transactions with PSD2, issuers have visibility of such information and can reject transactions in case of third-party deposits (with the right error message returned so merchants can have visibility of why this transaction was rejected).

**Important note:** as we all know, mobile card/wallet payment options are becoming increasingly popular nowadays, it is important that the 'verification of ownership' requirement also extends to these card options. →

For our industry, this measure is needed to help prevent fraud, money laundering, and address the responsible gambling problem in the right manner without hindrance to the overall customer experience.

### What about bank payments?

Open Banking was a game changer. Through Open Banking merchants are able to verify if the client is using their own means of payment.

However, there is more that can also be done for normal bank deposits/withdrawals, especially around banks in Europe, providing a Bank IBAN check feature.

### What is the bank IBAN name check feature?

Another feature that could help combat fraud, third-party deposits, and money laundering risks is the BANK IBAN name check feature.

We know such a feature exists in some EEA Countries like the Netherlands, France, and the UK but is not available in many other EU countries. For example, it does not yet exist in Belgium.

Such a service will allow merchants to confirm that the payee's name matches the name on the intended recipient's bank account. The IBAN Name Check will help avoid misdirected payments and reduces push payment fraud. This will give us and our customers confidence that any payments being made are going to (or coming from) the intended beneficiary.

**How does it work:** When receiving or sending payment, the merchant will send their own verified customer name + IBAN to the bank and the bank will send back 'match'/'no match'. The merchant will be able to decide whether to send payment or not based on this reply.

## Conclusion

The customer experience and having a seamless flow are important, as is mitigating risk related to fraud, money laundering, and harmful play. By promoting data sharing as part of a payment, it will be possible to check for third-party deposits in the background without impacting the client's experience. This would ensure the customer has a superior customer experience both during and after a transaction happens as he won't be asked for further documentation.

Only merchants and payment options that are able to strike the right balance will survive, as the alternative is either an unacceptable risk level or a very cumbersome/manual verification process for the customer.

In today's digital age, this is possible in practice if all the parties involved in the payment ecosystem collaborate by providing verified payment options.



[kindredgroup.com](https://www.kindredgroup.com)

**Kindred Group** is a digital entertainment pioneer bringing together nine successful online gambling brands – forming one of the largest online gambling groups in the world. Our collective purpose is to continue to transform gambling by being a trusted source of entertainment that contributes positively to society.

# Unlocking the Power of Digital Identity



*Digital identity is not a standalone product but a vital enabler of consumer objectives and business offerings.*

**Travis Jarae, Founder and CEO, Liminal**

# Consult Hyperion

## Using Digital Identity to Fight Financial Crime



**Steve** is an esteemed digital identity expert, advising banks, governments, and tech firms on governance, architecture, and implementation. He's contributed to various digital identity schemes worldwide, supports a number of industry initiatives and has authored papers and guides for organisations such as the DIACC.

Steve Pannifer ■ *Managing Director* ■ Consult Hyperion

Financial crime is a very complex topic. Criminals are clever, devious, and unpredictable. Whatever controls organisations put in place, criminals will find the weak spot and seek to exploit it for their own nefarious gain.

Identity sits at the heart of many crimes – criminals pretending to be someone else ('impersonation'), creating fictitious identities ('synthetic identity'), finding ways to assume the identity of normally law-abiding citizens ('identity theft') – as well as coercing naive or vulnerable people ('mules') to use their legitimate identities to unwittingly facilitate criminal activity.

It stands to reason therefore that secure digital identities (such as secure cryptographic digital credentials such as W3C verifiable credentials or ISO 18013-5 Mobile Driving Licences) will play an important role in the ongoing fight against organised crime. And those digital identities can help prevent crime in both the physical and digital worlds.

### Digital identity is so much better than current non-digital methods

There are many reasons why digital identity should be better than performing manual checks on physical documents.

First, cryptographic credentials are much harder to forge than physical documents. Perhaps the best example today is that of the passport which is usually both a physical and digital credential. Technology exists (and is widely used) to scan the physical document as part of an identity check, to facilitate remote onboarding and KYC

checks. But the physical part (or an image of it) is susceptible to tampering. Much better to use the secure cryptographic credential held in the chip.

Digital credentials can be issued more frequently than physical credentials. For example, in the UK for some years it has been possible to obtain a short-lived 'check code' to allow a car rental company to have temporary access to your driving record. It is not a big step to imagine the UK DVLA issuing a temporary digital version of your driving licence into a digital wallet, that is valid for just a few days. There is no need to be constrained by the costs and complexity of issuing physical documents.

In March 2020, FATF (the global money laundering and terrorist financing watchdog) issued [guidance on the role of digital in AML/CFT](#). They said that 'reliable digital ID can make it easier, cheaper, and more secure to identify individuals in the financial sector'.

### The digital identity landscape remains fragmented

Depending on where you live, you may or may not have something you would recognise as a digital identity, i.e. a wallet, account, or another digital tool that you can use to prove who you are in various contexts. There are a few places, such as the Nordics, where such systems exist and are used at scale. But these are still the exception rather than the rule. →



Over the past years, there has been a rapid rise in the use of document scanning solutions – requiring the user to scan a ‘photo ID’ with their mobile phone combined with a facial biometric check. These are not true digital identities. Instead, they act as a bridge from physical documents to the digital world. There is no denying that these solutions were hugely valuable during the pandemic enabling remote identification but they have their limitations. They require you to have the document with you – not a problem when locked down in the pandemic but more of an issue in more normal times. They also only provide a very limited set of data.

Consider the example of someone wanting to place a large bet on the World Cup final. They will need to prove their identity for AML purposes but potentially be able to prove their age, show the source of funds and pass affordability checks.

### Liability continues to be a stumbling block

The topic of liability continues to hamper the adoption of digital identity solutions. The idea that service providers rely entirely on third-party ‘identity providers’ who do not accept liability, to perform their identity checks is problematic.

Where that service provider is an AML reporting entity carrying the regulatory risk, then they will need to have control over the end-to-end process to manage their risk. Furthermore, the risk exposure of every service provider is different. It cannot be the case that a one size fits all identity verification will work across financial services, let alone across the economy.

Digital identity solutions can play an important role but they are not the whole answer. They can make the process digital. They can make the process more secure and reliable. But they will need to be augmented by background checks sufficient to address the service providers’ risk.

This is one reason why a credentials approach to digital identity makes sense. Rather than ask the customer for their ‘digital identity’ you ask them to share one or more verifiable credentials from their wallet, and these combined with other evidence enable the service provider to make its own determination about the customer.

### Orchestration is the answer

When you consider the plethora of use cases out there, the differing requirements of service providers and the fragmented sets of documents and data available for customers, it is clear that service providers need flexibility. Digital credentials in wallets are coming but it will be years before they are ubiquitous and standardised.

In the meantime, service providers will need orchestration capabilities to support whatever digitised or digital identities the customer may have.



[chyp.com](https://www.chyp.com)

**Consult Hyperion** is a UK and US-based consultancy specialising in secure electronic transactions, with over 30 years’ experience. They help global organisations take advantage of new technologies and regulatory changes in payments, identity, and future mobility. They design systems, offer digital innovation, and unblock technical issues, while their in-house Hyperlab team quickly prototypes concepts and delivers secure software.

# Intesi Group

## The Role Played by eIDAS 2.0 in the Development of the European Digital Identity Wallet and Payment Wallets



**Viky** is an international expert in the field of electronic signatures, digital identity, and digital transformation processes. She has been contributing to the impact assessment for the revision of the eIDAS Regulation in support of the European Commission, to establish a legislative framework for a secure, widely usable, and interoperable Digital Identity for the Digital Single Market – eIDAS 2.0.

Viky Manaila ▪ Trust Services Director ▪ Intesi Group

In modern times the wallet became the source of value to us – who we are and what we can buy. There are a lot of wallet solutions on the market: for payment, for payment combined with boarding passes and tickets, for all sorts of credentials, then why another wallet? What can a new European Digital Identity (EUDI) wallet bring? The answer is simple – **the identity** and many more pieces of information with a legal value that can be used in cross-border transactions within European space, no matter the country of issuance, to identify ourselves to public or private services.

eIDAS 2.0 is the proposal to amend the eIDAS Regulation (no. 910/2014) on electronic identification and trust services for electronic transactions in the internal market. The aim of eIDAS 2.0 is to achieve the target set in Europe's **'Path to digital decade'** – 80% of EU citizens being able to use a digital ID by 2030, to be able to prove who they are cross-border, to be able to give the explicit consent for sharing pieces of their personal information, to know exactly with whom they've shared personal information and for what purpose. This legislative intervention changes the EU framework for digital identity, introducing the EUDI wallet concept.

The EU's way for the digital transformation of our societies and economy encompasses in particular digital sovereignty openly, respect of fundamental rights, the rule of law and democracy, inclusion, accessibility, equality, sustainability, and respect for everyone's rights and aspirations. The EUDI wallet is human-centred, enforcing control and privacy, data minimisation, security, interoperability, and sharing of personal information based on explicit consent. We will know for sure with whom we share out data and for what purpose, as the wallet will have a dedicated

section for that, and those consents are available for consultation or withdrawal in time. This is a radical shift into the digital identity and authentication space, towards a decentralised model, user-centric, and individually controlled.

### What role will the EUDI Wallet play in the financial industry?

Identity is the bedrock for financial services and we have seen various initiatives in this space, like the Nordic countries' banks issuing digital identities (BankID Sweden, BankID Norway, NemID, MitID, FTN, iDIN) with a high adoption rate. However, these identities cannot be used cross-borders if a citizen needs to get a bank account in another country, for instance. There are also various remote identity verification solutions integrated into banking processes, collecting all sorts of documents and performing sophisticated checks of biometrics and liveness. This comes with an associated cost per transaction, in addition to the costs associated with customers' identity document preservation, encryption, and protection over a long period.

Here is where the EUDI Wallet enters the game, alleviating all of the complexity of onboarding customers or processing payments: being an electronic identification means with a high level of assurance, the EUDI Wallet can cut down the costs for KYC/AML, helping financial institutions fulfil specific regulatory requirements and build seamless online experiences. The eIDAS 2.0 highlights that the **financial services sector should accept the use of EUDI Wallet** for the provision of services where strong customer authentication for online identification is required by national or EU law or by contractual obligations. →

In addition to digital identity, through the EUDI Wallet, banks can also use other credentials (electronic attestation of attributes) with legal value issued by trust service providers or other banks, such as creditworthiness, fraud profiles, IBAN, and income/financial transaction data attestation. At the same time, banks can play the role of credential providers to the EUDI wallet, which can help with distribution and availability across multiple channels.

It is the time for banks to recognise the role they want to play in shaping the future of digital financial services and to decide on how they want to move forward as the ecosystem is in rapid development. The transition from physical wallets to digital wallets has already started, so the question is: are you a player or a spectator?

### Who are the early adopters?

While the eIDAS2.0 is following the legislative process, expected to be approved by the end of 2023, several consortia deploying large-scale projects have been selected for co-funding by the European Commission. EWC, NOBID, POTENTIAL, and DC4EU, composed of public-private organisations, have proposed various use cases in a cross-border environment, covering all European Member States. One in particular, the NOBID consortium, is focused on the payment means issuance and payment acceptance by retail or similar: instant payments and account-to-account transfers. The solution will build on the EUDI wallet usage as strong customer authentication, as well as transaction linking according to the PSD2 requirements.

The new European digital identity framework has a huge potential for banks, fintech, and payment providers: it will solve the historical problem of proving who we are on the internet, decreasing the frauds associated with identity theft or false claims. EUDI Wallet is the future of identification, going beyond making payments online or managing payment cards only.



[intesigroup.com](https://www.intesigroup.com)

An Italian private company, Qualified Trust Service Provider according to eIDAS Regulation, **Intesi Group** has more than 20 years of experience in cryptography, technology development, and trust services provisioning, serving customers from the highest regulated industries such as financial, biopharmaceutical, and healthcare.

# Mark Haine

## Potential Unintended Consequences of Implementing a Digital Identity Wallet



**Mark** is an engineer and entrepreneur who has focused his career on building solutions that enable business and mitigate risk largely in financial services. Mark has helped organisations navigate the complexities of securely enabling third-party access to data via APIs in tightly regulated environments.

Mark Haine ▪ Founder ▪ [consldr.consulting](https://www.consldr.com)

In 1999 Visa announced it was **'the year of the e-wallet'**. It wasn't until 2018 that **mobile wallet payments overtook payment cards by the number of transactions**. These two data points show that it can be notoriously difficult to predict how things will play out, not to mention when.

The European Commission under their Digital Programme has started a **pilot of the 'European Digital Identity Wallet' (EUDI)** which 'will provide a secure and convenient way for European citizens and businesses to identify themselves when needed for accessing digital services'.

There is certainly a vision and ambition for citizens to use a EUDI wallet to do things like check-in at the airport, rent a car, or open a bank account.

To move things forward having a vision and an ambitious plan is absolutely the right thing to do but as part of that plan, it is very important to try to spot where challenges may lie and plan to avoid, work around, or meet them head-on with solutions. This article tries to provide a list of challenges that may need to be overcome before the stated target that **'80% of (European) citizens have access to digital ID' can be realistically achieved**.

### Increased identity theft

Increasing the convenience of carrying and presenting identity information makes it much better for citizens, and the businesses they are dealing with, when things are going well. However, making it easier to share digital identity credentials also makes it easier to over-share with a relying party that wishes to use data in a way that

the end-user has not agreed to or, much worse, easier to share digital identity information with a fraudster. It could well be that one of the biggest risks arising from the EUDI Wallet is that it makes it easier for fraudsters to access citizens' digital identity credentials by simply tricking them.

In some ways, this may be compounded by using the wallet. Part of the reason a wallet is good is that it reduces potential abuses by legitimate businesses by making the tracking of user behaviour harder, unfortunately, it quite probably also makes tracking and stopping fraudsters harder too.

### Security, privacy, and tracking

The digital wallet may reduce tracking by credential issuers, but concerns about using digital identity persist among citizens. The prevalence of cyber security incidents and online influencers warning about the potential tracking capabilities of digital IDs have only amplified those concerns, ultimately it is easier to track the use of digital IDs than track the use of physical IDs. While the wallet architecture is a response to web tracking and gives end-users some control of their credentials, it may shift the problem to different components of the technology stack, such as network operators, wallet providers, or mobile OS providers. It is uncertain whether the wallet-based architecture will really mitigate tracking, but it offers a potential solution for consumers who have grown wary of web tracking and abuse by big players. →

## Digital divide

Another probably unintended consequence is that a disproportionate burden falls upon people in lower socio-economic groups. While making digital journeys easier and safer is the overall goal it seems likely that the use of these 'easier' journeys will, in reality, be easier for people who already have the skills and appropriate devices, and already have one or more existing sources of strong identity (like a passport). The unintended consequence here is that there is bias baked into the assumptions of the programme that further expands the existing digital divide more, increasing discrimination against people who for whatever reason already struggle with digital journeys.

## Incompatibilities

When building a multi-party ecosystem, the reputation of the overall system is quite strongly tied to the interoperability of many parties. If any one entity in the ecosystem implements a change that renders it incompatible at a technical level with other parties, then the impact will be much wider than the single party, and there will be dissatisfaction with the ecosystem in the mind of impacted consumers.

In the case of the EUDI ecosystem, it is anticipated that there will be many issuers, relying parties, and wallet providers. It is highly likely that technical incompatibilities will exist, sometimes transient but also potentially for extended periods as multi-party troubleshooting takes place. This will inevitably impact the utility and reputation of the EUDI ecosystem as a whole. It also seems likely that fallback mechanisms will have to be designed into the relying party processes and systems for when people present themselves and there is a glitch that cannot be resolved in a timely fashion, for example when presenting credentials that are needed to board a plane.

The fallback measures are likely to be more time-consuming and costly and could have knock-on effects for all concerned.

## Innovation

Delivery of a functioning digital ecosystem that works across borders and business sectors that reduces the risk for legitimate

participants is a tall order. Doing it in a way that is sufficiently stable to become the primary channel will require an unprecedented level of standardisation and operational stability. Once that stability is achieved changes by implementers will need to be performed very carefully, and change to the standardised interfaces will be very hard.

This necessary operational stability will act as a significant impediment to future change (and therefore innovation) and unless it turns out that the solution presented is pretty close to 'the right answer' this could have a significant detrimental impact on the ability to innovate going forward.

## Business model

The cost of interacting with the EUDI ecosystem will be a barrier for some businesses, there will need to be additional equipment, software, or services to interact with the EUDI ecosystem whether they integrate themselves or subscribe to a service provider to help. There is also the potential for smaller businesses to find that accepting digital identity is not cost-effective if their transaction volumes or margins are not enough to cover the overheads.

Maintenance, upgrades, and dealing with incidents and disputes will also incur a cost but it remains unclear how that may be covered. Despite the likely macro benefits of digital identity, the unresolved business model for using EUDI Wallets may have unintended consequences for some market participants, resulting in some business entities losing out.

## Success?

We have one measure for success in the '80% of citizens have access to digital ID' statement but perhaps a greater success was if the use of strong digital identity via a EUDI Wallet were to overtake the inefficient, insecure, costly, and generally annoying assurance processes we have to endure today. Let's keep discussing how we can address these (and other) consequences and hope we get there in less than the 19 years it took payment wallets to overtake cards.



[considrd.consulting](https://www.considrd.consulting)

**considrd.consulting** is a specialist consultancy founded by Mark in 2020 that focuses on strategy, architecture, and engineering of Digital Identity, transformation, and security concerns and has supported clients in many countries.

# Liminal

## Unlocking the Future of Digital Identity: the Key to Seamless Customer Experience and Business Growth



**Travis Jarae**, founder and CEO at Liminal, is a digital identity and technology thought leader. He's passionate about building a community dedicated to solving the challenges of digital transformation. With leadership roles at Google, Deloitte, and Citi, Travis has a keen eye for helping organisations navigate growth market opportunities and strategically allocate resources.

Travis Jarae ▪ *Founder and CEO* ▪ Liminal

In today's world, digital identity and verifiable credentials are becoming increasingly important in the delivery of products and services. Liminal believes that digital identity is not a standalone product but a vital enabler of consumer objectives and business offerings. These capabilities are increasing in value to organisations and will enable a smooth transition from the current Web2 model to a decentralised Web3.

Digital identity refers to the digital representation of an individual or organisation, and verifiable credentials provide evidence of identity attributes, such as licences, memberships, or employment history. In the current digital identity model, individuals must create and maintain multiple accounts, passwords, and personal information across various websites and services. This leads to a fragmented and cumbersome experience that can lead to data breaches and security risks. Unfortunately, the model creates a poor customer experience because of the need to enrol and re-provide identity information for every new website or service.

Our recent research found that security is the greatest priority when onboarding and 42% of consumers have abandoned an account application due to friction. One particularly acute area where friction is problematic is in digital onboarding, especially for financial services accounts with Know Your Customer (KYC) and anti-money laundering (AML) requirements for ensuring that a customer is adequately verified. Consumers have become accustomed to onboarding flows in consumer-facing applications that have not had the rigorous requirements for KYC and AML checks, and therefore are affronted by requests for proof of identity for financial services applications that they don't experience in other forms of account opening.

There are exciting efforts underway to build a drastically different future, with emerging models such as Personal Identity Ecosystems (PIEs), Identity as a Service (IDaaS), eIDs and identity wallets, and self-sovereign identities (SSIs). These models aim to move digital identity from siloed, privately-held databases to open networks where individuals and businesses can maintain their identity and credentials in one place and then reuse them wherever they go.

Adopting reusable digital identity and verifiable credentials is poised to bring significant advantages to both individuals and organisations by eliminating the need for constant re-enrollment and re-verification, resulting in substantial time and cost savings. This enables users to share their verified identity attributes across various services and applications, creating a seamless and secure experience that enhances customer satisfaction. Given the growing consumer demand for streamlined, personalised, and privacy-protecting interactions, organisations recognise the need to embrace these innovative technologies to remain competitive in the market.

A major obstacle to the widespread adoption of digital identity and verifiable credentials is the need for interoperability and adherence to common standards and frameworks across different systems. This requires businesses to have a comprehensive understanding of the technical, legal, and regulatory aspects and ensure adequate privacy and security measures. To achieve this, organisations must collaborate with stakeholders to establish a shared language of compatible standards and protocols to ensure universal adoption and interoperability. →



Furthermore, shifting from a traditional siloed identity model to a more open and interoperable network has significant implications for businesses. With the adoption of reusable digital identity and verifiable credentials, organisations will be able to provide a seamless and personalised customer experience that is more secure and efficient. However, this transition requires significant changes to existing back-end operations and underlying technologies, including authentication protocols, identity providers, and authorisation frameworks.

This change poses new security concerns as sensitive identity information will be shared across multiple services and applications. Organisations must ensure the privacy and security of personal data by implementing robust security measures, such as data encryption, secure data storage, and access management. Adopting industry best practices, guidelines, and standards, such as ISO/IEC 27001 or NIST Cybersecurity Framework, can help businesses establish a secure and resilient digital identity and verifiable credentials ecosystem.

Reusable digital identity and verifiable credentials are key to building a secure and trustworthy Web3, where users can seamlessly interact across decentralised applications without compromising their privacy or security. As the market for these solutions grows, organisations must adapt to meet customers' evolving demands. However, this shift from a siloed identity model to a more open and interoperable network requires significant changes to existing back-end operations, underlying technology, and security practices, which poses challenges for businesses. Nonetheless, with careful planning and stakeholder collaboration, businesses can overcome these challenges and reap the benefits of a more streamlined, secure, and efficient digital identity ecosystem. At Liminal, we are committed to staying at the forefront of emerging market trends and helping organisations navigate the complex landscape of digital identity and verifiable credentials.

**Figure: 2023 Liminal Digital Identity Landscape**

The Digital Identity Landscape tracks emerging trends and technologies, providing enterprises with valuable insight into the direction of the industry and helping to shape next-generation strategies. Identifying and tracking more than 120 product features mapped to 32 solutions segments across more than 2,000 key players in the market makes it the most comprehensive digital identity market intelligence tool available globally. This allows senior executives representing small and large businesses to identify opportunities for growth and expansion, as well as potential areas of risk.



[liminal.co](https://liminal.co)

**Liminal** is a strategy advisory firm serving digital identity, cybersecurity, and fintech firms, as well as private equity and venture capital investors, helping leaders make decisions at all stages. Our clients include business leaders, investors, and government officials seeking to invest in the next-gen of digital identity platforms. We offer solutions for evolving market dynamics, growth strategies, M&A opportunities, and deal flow optimisation. We guide clients in navigating complex digital transformation challenges by showing them how to reach their destination.

# Achieving Seamless UX, Robust Security, and Compliance in Digital Onboarding & KYC



*Companies that can strike a balance between the friction required for effective verification and a smooth onboarding experience can gain a competitive edge.*

Michael Ramsbacker, Chief Product Officer, Trulioo

# Ping Identity

## Know Your Customers: the Power of Digital Identity



**Maya Ogranovitch Scott** is a Solution Marketing Manager for Ping's financial services solutions. She is passionate about leveraging the power of identity to help enterprises deliver exceptional customer experiences that are simultaneously secure and seamless.

Maya Ogranovitch Scott ■ *Solution Marketing Manager* ■ Ping Identity

Do you know who your customers are? This sounds like a trick question, but it isn't. Although organisations must have Know Your Customer (KYC) and Anti-Money Laundering (AML) checks, the certainty around identity isn't as high as it should be. For financial services organisations, failure to verify identity carries heavy fines and reputational costs. According to **UK Finance**, instances of credit card ID theft (new cards using stolen identities or account takeovers) were up 101%, with a reported gross loss of GBP 21.4 million for H2 2022.

Identity verification is a powerful capability that helps defend against new account fraud, application fraud, card ID theft, and account takeover. When utilised with best practices, organisations can protect themselves and their customers while delivering delightful digital experiences.

### Use cases throughout the customer journey

Leveraging verification throughout the customer journey helps manage financial, identity, and compliance risks.

#### Account opening

When customers initiate their first interaction, verifying identity against an official document should include matching the name and face on the document and verifying the document's validity. Verifying validity decreases the likelihood of fraudsters opening accounts with stolen/synthetic identities.

#### Borrowing money

Verifying identity should be a prerequisite for releasing borrowed funds. Whether part of the account opening or re-verifying again before allowing access to funds, proofing at this point in the customer journey significantly reduces money misappropriation.

#### Wire transfers

Many financial institutions require MFA before allowing large transfers. However, re-verifying the identity at this point is a better way to stop fraudulent transfers initiated as part of an account takeover.

#### In-person check cashing

Digital identity proofing stops certain types of fraud that occur in bank branches.

Whether the individual is an existing customer or not, verifying identity can mitigate most in-person check fraud. Ping estimates that identity verification reduces this type of fraud by over 90% when implemented correctly. →

## Service and support

Legitimate customers require support and identity verification helps ensure that the support agent doesn't accidentally aid a fraudster in a crime. For password resets, account closures, and disputes it's imperative to know that the identity of the person requesting support matches the identity of the customer who owns the account. This protects against account takeover and stops fraudsters before they create lasting harm.

## Identity proofing best practices

Not all identity verification solutions are equal. A strong service, like PingOne Verify, should allow you to quickly, reliably, and confidently ascertain two things: 1) the real-world identity exists, and 2) the person undergoing the proofing is the actual owner of that identity. The verification process should be done in real-time and be as easy as presenting a physical ID.

Biometrics (voice and facial recognition) is a key differentiator. The service should be tested for racial bias, accurately match all skin tones, and verify physical and digital government-issued ID validity. Finally, a good identity verification service should match the face of the user to the face on the document, performing a liveness check. The liveness check prevents spoofing by confirming that the individual is alive and physically present during the verification.

## Introducing decentralised identity

Decentralised identity is an approach to IAM that allows users to control their identity information. Sometimes referred to as self-sovereign identity, it eliminates the need for users to provide unnecessary amounts of personal information to access a service. Organisations issue users' verifiable digital credentials that are stored in a digital wallet. Users present their credentials to organisations that verify the information instantly without contacting the issuer.

Decentralised identity helps financial institutions comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations

by using robust verification mechanisms to create an immutable record, reducing the risk of fraud, and improving the accuracy of compliance checks.

PingOne Neo is Ping's new decentralised identity solution. Neo verifies IDs, documents, and identity claims and issues digital credentials based on those. Users can share credentials with organisations to quickly and effortlessly prove who they are.

## Conclusion

Implementing verification and credentialing at the appropriate moment in the customer lifecycle is critical. Most customers expect to verify their identity at least once, but it should only happen occasionally, even if the process is easy. ID proofing is a valuable component of a larger threat protection strategy, and it works best when integrated with other fraud detection, authentication, and authorisation tools. This integrated approach allows organisations to challenge users when needed without overwhelming them with unnecessary security steps. Getting the balance right may take trial and error, but the results are worth it.

[Click here for the company profile](#)



**Ping Identity** delivers a comprehensive set of identity and access management services. Customers may choose any or all they need without vendor lock-in. Our platform makes it easy to integrate services with speed and precision, streamline multi-vendor architectures without custom coding, and explore and optimise journey flows with minimal disruption.

[pingidentity.com](https://pingidentity.com)

# Trulioo

Michael Ramsbacker, Chief Product Officer at Trulioo, discusses how businesses can leverage layered identity verification to onboard the right customers.



**Michael** has more than 20 years of experience in the strategic execution of product strategies, particularly for the business-to-business technology industry. At Trulioo, he oversees the launch of new digital identity verification solutions and services.

Michael Ramsbacker ■ Chief Product Officer ■ Trulioo

## What is a layered approach to digital onboarding, and how does it help prevent fraud?

Robust digital onboarding requires a layered stack of capabilities working together to rapidly onboard legitimate users while creating barriers for fraudsters. Given the complexity of identity verification and regulations around the world, a business can't rely on any single technique to meet its onboarding objectives.

For example, a data source check might not adequately verify people in countries with thin data coverage, so businesses can add document verification as an extra layer. That layered approach adds a point of good friction, identifying fraudsters while letting legitimate actors through.

“ To achieve smooth, secure digital onboarding, companies should leverage an identity platform with the expertise, tools, and layered capabilities to optimise verification.

A layered stack of verification techniques can help businesses minimise the risk of fraudulent activities – such as account takeovers, identity theft, and fake accounts – and safeguard customers' sensitive information. Ultimately, layered verification helps to filter out bad actors while ensuring fast, convenient onboarding for good actors.

## What are the key components of a layered approach to digital onboarding, and how do they work together to enhance security and prevent fraud?

A layered approach to digital onboarding involves multiple active and passive processes to filter out the good actors from the bad. A typical verification process will collect personally identifiable information (PII) – such as name, date of birth, and address – from individuals and articles of incorporation from businesses. Meanwhile, passive data is collected in the background to confirm critical network and device information, such as an IP address. Those components must work harmoniously to establish strong fraud prevention measures without compromising customer onboarding experiences.

## What role do artificial intelligence and machine learning play in a layered approach to digital onboarding, and how can they be used to detect and prevent fraud?

Artificial intelligence and machine learning (AI/ML) are revolutionising identity verification, helping to optimise onboarding at a scale humans can't. AI/ML can find patterns in vast amounts of data – such as PII, network information, and geospatial analysis – to establish accurate customer risk profiles.

For instance, during manual document verification, a person can look at a picture of a driver's licence and try to figure out if it's real or fake. People do a reasonably good job but probably won't catch more sophisticated fake identity documents. →

AI can play a dual role in identity verification by enhancing security and delivering a better user experience. Using AI/ML, companies can quickly identify high-risk users and prioritise them for additional verification while letting low-risk individuals through.

While some identity platforms have integrated AI/ML on an individual service level, the future of identity verification is even more promising as AI evolves to build hyper-targeted workflows tailored to each user. AI's role in preventing fraud is becoming essential, enabling smooth customer experiences and streamlined onboarding.

### What challenges do organisations face when implementing a layered approach to digital onboarding, and how can they be overcome?

Finding the right combination of verification methods can be a challenge for any organisation. Many companies use multiple vendors for individual verification services, which can limit oversight and control of the process and create inefficiencies. Identity verification isn't static, and companies need solutions that can adapt to changing fraud risks, regulations, and business needs.

Those challenges are amplified for companies with global footprints. Each country has its own set of regulatory requirements, identity verification sources, and best practices. Using an identity platform with global reach and localised expertise is crucial to finding the right layered approach for each country.

Agile capabilities become essential to a smooth onboarding process. Those companies that can strike a balance between the friction required for effective verification and a smooth onboarding experience can gain a competitive edge.

### How can organisations measure the effectiveness of a layered approach to digital onboarding, and what metrics should be used to evaluate success?

In this changing economic environment, more companies are focusing on onboarding the right people. Organisations can get a sense of how much it costs to onboard the right customer by factoring in the amount spent filtering out the bad actors from the good. Everything is a leading indicator, so businesses need the right instruments to accurately measure those numbers.

Some helpful metrics include:

- The number of active versus passive verification techniques used;
- The number of bad actors who were stopped;
- The amount spent on direct vendors, staff, development, and resources.

To achieve smooth, secure digital onboarding, companies should leverage an identity platform with the expertise, tools, and layered capabilities to optimise verification. Those platforms can also provide a vision for broader AI implementation to accelerate workflow optimisation.

By partnering with a global identity platform, businesses can ensure enhanced customer onboarding experiences, setting the stage for long-term success.

[Click here for the company profile](#)

**Trulioo**

[trulioo.com](https://trulioo.com)

**Trulioo** is the identity platform global businesses turn to for growth, innovation, and compliance. The platform helps companies achieve regulatory compliance, reduce risk, and expand their businesses by enabling the verification of more than 5 billion people and 300 million businesses across 195 countries.



# IDVerse, an OCR Labs Company

## Generative AI in IDV: the Good, the Bad, and the Necessary



Daniel is the Co-founder and CPO of IDVerse, an OCR Labs Company. Dan is a serial entrepreneur, and along with co-founder Matt Adams, launched his third startup. Dan has developed patent-pending machine learning technology that can read and understand languages used by 98% of the world's population whilst achieving Zero Bias AI. He leads the product team at IDVerse to ensure that clients onboard customers smoothly and remotely, are compliant and stop identity fraud.

Dan Aiello ■ CPO ■ IDVerse, an OCR Labs Company

Generative AI – a type of artificial intelligence technology through which content such as text, images, audio, and video can be produced via written prompts – has become a global sensation in just a matter of months. Even outside of the tech industry, you'd be hard-pressed to find someone who hasn't heard of ChatGPT, DALL-E, MuseNet, or any of the other generative AI programs that have recently been released to the public at no cost (for now).

Leaders in sectors ranging from academia to film and television have spoken about the consequences this technology could have in the hands of bad actors. Concerns about plagiarism, copyright infringement, and disinformation have all leapt to the forefront since the beginning of the year.

Others have noted how generative AI has been a boon to marketers and businesses seeking to create high-quality content at scale, improve the user experience, and increase the efficiency of development workflows.

Fewer people, however, are talking about how generative artificial intelligence has completely disrupted the identity verification (IDV) and fraud detection landscape. In other words, what would 'the ChatGPT of IDV' look like?

### Going deep(fake)

The most advanced IDV solutions use generative AI and neural networks along with biometric data – such as a person's face – to authenticate users seeking to perform a high-risk activity like opening a bank account or initiating a financial transaction. The requirement, therefore, is to create solutions that stay ahead of bad actors by using the technology better than they do.

Advanced fraudsters use what's called synthetic media to steal identities. More commonly known as 'deepfakes', this technology uses generative AI to create convincing image, audio, and video hoaxes. Deepfakes often work by transforming existing content where one person is swapped for another, and they can be incredibly hard to detect with the unaided human eye.

The ease of creating a convincing deepfake can vary depending on various factors, such as the quality of the source material, the complexity of the algorithm used, and the creator's level of technical expertise. Unfortunately, the availability of powerful, open-source machine learning software has had a proliferating effect on identity fraud – it is becoming far easier for individuals with only basic-level technical knowledge to create convincing deepfakes.

An additional contributing factor to the rise in identity fraud is the profusion of training data. Creating a convincing deepfake requires a large dataset of images or videos to train the algorithm. With virtually limitless content available for the taking on social media platforms, there is an abundance of material online.

Computing capacity is yet another variable in the fraud equation. The production of deepfakes requires a significant amount of processing power, which has become more accessible with the availability of cloud-based computing services and affordable graphics processing units (GPUs). →

Faced with these mounting threats, a robust IDV solution is no longer a nice-to-have item, but rather an essential part of safely doing business. Manual techniques are no longer fit for purpose; companies need to invest in AI-driven IDV software to keep themselves and their users safe.

### Data privacy policy and using generative AI for good

Happening concurrently with the upsurge in identity fraud is a growing trend of regulations focused on biometric data privacy. With fingerprints, iris scans, and facial recognition now commonly used as part of businesses' authentication processes, concerns over privacy and misuse have led to increased regulatory attention.

A couple of the most significant examples of biometric data privacy regulations are the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the US. These policies set strict requirements for the collection, use, and storage of personal data and mandate that companies implement adequate security measures to protect it.

The Biometric Information Privacy Act (BIPA) in the state of Illinois, first enacted in 2008, has also been gaining renewed attention. Significantly, BIPA prohibits companies from using biometric data collected from users to train their machine-learning algorithms and provides a mechanism for users to pursue litigation for privacy rights violations.

With such regulations placing strict guardrails on how biometric data can be used, IDVerse has instead trained its technology on vast datasets of AI-generated synthetic faces. This technique allows our learning model to improve its accuracy in identifying – and locking out – bad actors attempting to gain access using deepfakes.

Here are five steps for incorporating generative AI into IDV systems development:

- 1. Gather a diverse dataset of synthetic media:** generate a large dataset of unlabelled synthetic media produced by generative AI systems, including images, videos, and audio recordings.
- 2. Label the dataset:** thoroughly annotate the synthetic media dataset to identify the type of deepfake, the system used to generate it, and any other relevant information.
- 3. Train the identity-proofing system:** Use the labelled dataset to train the identity-proofing system on how to spot deepfakes created by generative AI systems.
- 4. Evaluate the performance of the system:** test the trained system on a different dataset of synthetic media and evaluate its performance using a variety of advanced metrics.
- 5. Refine the training process:** based on the outcomes of the evaluation, refine the training process to improve the accuracy of the identity-proofing system.

Another key element of the development process is encoding the ability to share learnings, which is becoming imperative in the fight against synthetic media deployed in high-volume flash attacks. Using advanced deep neural networks and shared fraud hubs, IDV systems can apply knowledge learned in one part of the network across the entire ecosystem of users.

It's clear that the generative AI arms race between would-be fraudsters and businesses who collect and accumulate user data is only just beginning to heat up. The stakes have never been higher – and companies need to prepare by implementing effective, efficient IDV solutions.

[Click here for the company profile](#)



[idverse.com](https://idverse.com)

IDVerse, an OCR Labs Company helps you quickly scale your business globally. Our fully-automated solution verifies new users in seconds with just their face and smartphone – in over 220 countries and territories with any ID document – without the burden of human intervention. For more information, visit <https://idverse.com/>

# Ekata, a Mastercard Company

With recent economic uncertainty leading to banks and fintechs investigating new sources of revenue among consumers, Micheal Pettibone from Mastercard shares how can these turn customer trust into revenue.



**Micheal Pettibone** is a technology executive with over 20 years' experience in Identity & Authentication. He is Senior Vice President, Identity Solutions at Mastercard leading global strategy, innovation & growth. Prior to Mastercard, Micheal spent over a decade in leadership roles at Oracle developing and expanding their Identity & Access Management business. Prior to that, Micheal was at PwC advising organisations on Identity & Security. He received his MBA & MSIS from Baylor University and resides in Dallas, TX.

Micheal Pettibone ■ Senior Vice President, Identity Solutions ■ Mastercard

## Would you say it is true that recent economic uncertainty has led to banks and fintechs investigating new sources of revenue among consumers?

In addition to serving existing clients, financial institutions and service providers are also looking to acquire new customers, including the underbanked – those without sufficient access to financial institutions. With limited banking or credit history to refer to, these customers often become a blind spot to traditional KYC and credit-driven identity verification practices, which forces financial institutions to remediate with high-friction identity proofing solutions such as document requests or ID card scans. Mastercard's identity solutions offer low or no friction to prove a new customer is who they say they are while keeping bad actors from opening an account and further engaging on the platform.

## Are there any new or evolving fraud trends emerging in the financial services industry due to the market shift? Can you provide some examples of those trends and how they are impacting the bottom line of banks and fintechs?

The digital economy is growing rapidly as technology continues to remove borders and barriers. As the digital economy grows, so too does uncertainty and more sophisticated fraud. Sophisticated fraud such as account takeover impacts consumers and businesses alike. The growing threat of synthetic ID fraud is also wreaking havoc across the ecosystem. Using a combination of valid or generated information, fraudsters attempt to open new accounts or even apply for lines of credit. Identity fraud is one of the greatest threats to building a secure, seamless digital economy. In the United States alone, identity thieves

steal more than USD 5.8 billion a year with 25% of victims reporting a loss, according to the Federal Trade Commission (FTC). This number is expected to grow, as fraudsters evolve their tactics and people conduct more of their day-to-day lives online.

“ Combining behavioural biometrics, identity elements, and data insights helps trust on both sides of a digital interaction.

## What do you think trust means to consumers today as they attempt to open new accounts with a specific bank or fintech in this volatile market?

This is a great question. It is true that today's consumers place a high value on convenience. At the same time, they expect their financial services and payment providers to keep them and their assets safe. Consumers expect technology to work with limited friction, for their data to be shared safely and securely, and to receive their goods or services quickly. This is not only a point of convenience, but a business imperative for financial institutions. When a customer has a poor experience with a bank, they will seek an account elsewhere. Studies show that nearly half of consumers would take their business elsewhere after just one bad online experience. Financial institutions need smart, secure, reliable tools to verify individuals online and establish trust. →

It is no secret that consumers are choosing to open new accounts online, making it a challenge for banks and fintechs to know who their customers are. Friction is a term we hear often when consumers are attempting to open new accounts. What impact do you think friction has on the potential loss of customers and their lifetime value when opening accounts online?

Consumers are looking for both speed and security in their digital interactions. Financial institutions that achieve the right balance between reducing risk and meeting consumer expectations will see the most benefits across the board. The key is striking the right balance. Approving bad actors cost businesses USD 6.7 billion in losses in 2021 according to one Javelin study. While some estimate the scope of false decline loss to cost merchants a whopping USD 643 billion. Applying too much friction can frustrate the consumer leading to an average form abandonment of nearly 68% based on findings from WPFForms. However, intelligent friction prioritises both experience and security. Both are critical to growing a healthy business. Businesses looking to gain more genuine new and retain existing customers will leverage intelligent friction to do so.

What strategies and tools would you recommend banks and fintechs put in place to help augment their KYC (Know Your Customer) process for a better customer experience?

At Mastercard, trust is our business, and we are committed to making the global ecosystem seamless, safe, and secure for everyone, every transaction, and every interaction. From opening a new account to logging in, to transacting, we're protecting all aspects of the consumer's online journey.

Our multi-layered approach to security utilises enhanced behavioural biometrics and machine learning and works behind the scenes to create a secure, trusted source of truth. This delivers greater confidence in decisions without sacrificing user experience. Mastercard Identity Check Insights, for example, draws on the safe exchange of identity data leveraging industry standards, machine learning, and fraud prevention programs to help merchants and banks confidently know who their customers are and promote secure digital commerce. Our identity technologies also play a critical role in consumer transactions using technologies like biometrics to help people prove they are who they say they are.

Are there any other thoughts and recommendations you want to share to help banks and fintechs as they continue to evolve their strategies to service their customers while combating fraud?

Financial institutions can provide seamless experiences, drive growth, and foster loyalty by adopting a multi-layered approach to security. Tools like Mastercard's Open Banking for Account Owner Verification service, for example, arm fintechs with the information they need to verify a new customer is who they claim to be while also meeting customers' needs for security and transparency.

This helps build the very trust that is needed in an increasingly digital world. Combining behavioural biometrics, identity elements, and data insights helps trust on both sides of a digital interaction. This is central to building a vibrant economy that works for everybody, everywhere.

[Click here for the company profile](#)



[ekata.com](https://ekata.com)

**Ekata**, a Mastercard company, empowers businesses to enable frictionless experiences and combat fraud worldwide. Our identity verification solutions are powered by the Ekata Identity Engine, which combines sophisticated data science and machine learning to help businesses make quick and accurate risk decisions about their customers. Using Ekata's solutions, businesses can validate customers' identities and assess risk seamlessly and securely while preserving privacy. Our solutions empower more than 2,000 businesses and partners to combat cyber fraud and enable an inclusive, frictionless experience for customers in over 230 countries and territories.

# Caf

## Leveraging Optimal KYC and KYB Processes to Combat Fraud and Drive Revenue Growth for Financial Institutions



**Jason Howard** is the CEO of Caf and a longtime identity industry executive. Prior to joining Caf, Jason served in the leadership team at Ethoca, the world's first collaborative fraud prevention network, which was acquired by Mastercard, where he was responsible for driving global revenue growth and customer success.

Jason Howard ▪ CEO ▪ Caf

Due to the highly regulated nature of the financial services industry, it is imperative for firms operating in this sector to strictly follow comprehensive Know Your Customer (KYC) protocols when welcoming new users. Similarly, when establishing relationships with new business clients, meeting the Know Your Business (KYB) requirements becomes crucial.

Having proper KYC and KYB processes and solutions in place is vital to fighting fraud and preventing financial crimes such as money laundering. But it is also difficult to conduct KYC checks in a digital environment where fraud and cyberattacks are so rampant. Financial institutions must be able to accurately verify the identity of all new customers while being able to detect and stop fraud.

KYC compliance is often a burden for organisations, requiring manual intervention and being rife with inefficient processes. Firms can ultimately waste a lot of money and countless internal resources with inefficient KYC processes.



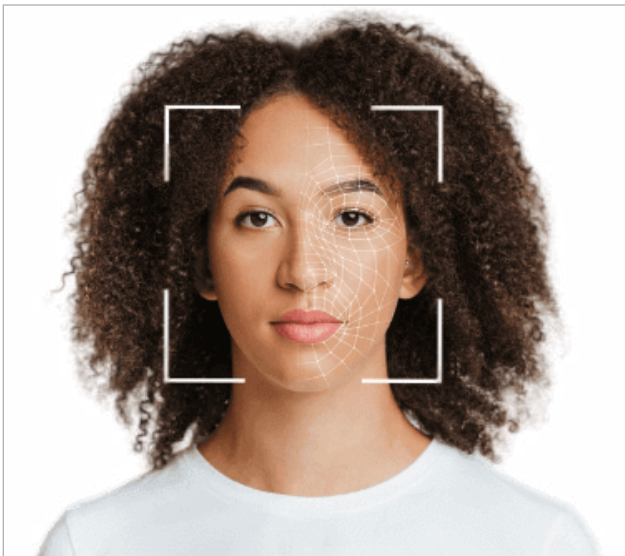
That said, here are 5 main pillars financial services firms should follow when it comes to KYC to fight fraud and grow revenue:

- 1. Accuracy:** Whatever processes or solutions you have in place must be accurate in validating all PII and verifying that whatever documents are submitted are legitimate and not faked with a high degree of certainty.
- 2. Compliance:** The KYC process should also ensure all applicable regulatory requirements, such as AML regulations, consumer data privacy laws, and others are being met.
- 3. Speed:** Firms should have processes in place to quickly authenticate the customer's identity, complete the verification process, and provide a clear result.
- 4. User experience:** Likewise, you need to offer a seamless and user-friendly experience for customers, who may become frustrated and abandon the process if faced with too many onerous steps to complete. It should be accessible and easy to use, regardless of the device or platform.
- 5. Security:** Finally, the solution should ensure the security of customer data, with robust security measures in place, such as encryption and multi-factor authentication, to protect against data breaches and unauthorised access.

KYC is not merely a compliance function, but a business driver as well. Having robust KYC protocols in place helps to onboard more customers quicker and keep them safe. Striking the right balance between safety and user experience when it comes to KYC means you will have higher user satisfaction and drive revenues. →

Luckily, any business can create optimal KYC processes. The use of the latest technologies combined with continuously improved AI algorithms and ML models makes it easier than ever before to validate identities, manage new and old users, enhance risk-decisioning, and ensure compliance with changing regulations at lower costs.

When it comes to KYB, a common issue that many organisations face is that too many lump KYB in with Know Your Customer (KYC) processes. KYB compliance should be its own discipline with its own processes to ensure optimal outcomes.



For the optimal KYB experience, financial services firms need to combine the right technology with reliable data sources. This can include implementing technology that can automatically extract data from documents and pre-fill required forms with that information, which not only increases operational efficiency but reduces the manual input required by the user. That information should then be automatically checked against the government and other relevant proprietary and third-party databases to ensure the verification of every business stakeholder. This part is critical; you cannot just rely on self-reported data when it comes to KYB.

It's also imperative to do thorough checks on each ultimate beneficial owner (UBO) related to the business. A UBO is any owner or stakeholder in a business. When onboarding a new business client, you must be able to accurately identify and verify all UBOs and conduct an end-to-end verification of every stakeholder. Ensure all information they provide matches public and private databases and generates risk scores for each individual. Fully vetting UBOs means you will be able to better prevent fraud and financial crime as well as meet all statutory requirements.

The use of the right technologies combined with proper processes makes it easier to validate identities, manage new and old users, enhance risk-decisioning, and ensure compliance with changing regulations quickly, at a lower cost, and without the need to rely heavily on your dev team.

[Click here for the company profile](#) 



[caf.io](https://caf.io)

**Caf** offers identity verification, onboarding, and authentication solutions to digital businesses to help secure their customers' journey. Our comprehensive suite of identity solutions enables the verification of individuals and businesses and is designed to accommodate the unique requirements of both regulated and non-regulated businesses.



# The Benefits of Emerging Tech in Transaction Monitoring for FIs and Crypto Providers



*It's important to approach the implementation of AI, ML, and NLP technologies with a critical eye and a focus on transparency, fairness, and accountability. By doing so, it is possible to harness the power of these technologies while minimising potential risks and drawbacks while optimising the expected return on investment.*

Alan Morley and Fanny Ip, Huron

# Regulatory Landscape and Regtech Trends



*The KYC Expert Group recommends the introduction of a harmonised EU-wide access mechanism that would enable financial institutions to access any official register, ideally through an interconnected portal, without any additional registration requirements at a national level.*

**Thomas Egner, Secretary General, Euro Banking Association**

# Euro Banking Association (EBA)

## Streamlining Low-Risk Situations and Overcoming Other Roadblocks: the Journey to a Uniform European KYC Experience



**Thomas Egner** is Secretary General of the Euro Banking Association, where he supports over 160 member institutions in pursuing a pan-European vision for payments. Prior to this, Thomas was responsible for defining and developing clearing and settlement strategies at Commerzbank. He represented this bank in the EPC and the German banking community in SWIFT and ISO committees as well as on the EBA CLEARING Board.

Thomas Egner ▪ *Secretary General* ▪ Euro Banking Association (EBA)

Know Your Customer (KYC) due diligence has become an integral part of the financial system. All customers of financial institutions, whether they are private individuals or legal entities, such as corporates, are subject to comprehensive KYC processes. These are aimed at ensuring that banks understand each customer's business profile, their financial activity, and the potential risk exposure they represent with regard to money laundering (AML) or financing of terrorism (CFT). However, as each multinational corporate is painfully aware, such KYC processes differ from bank to bank and, even more so, from country to country. This lack of harmonisation puts a significant financial and operational burden on all market participants that are active across the European Union.

### Negative implications of diverging KYC requirements

The problem is caused by diverging regulatory requirements for KYC processes across Europe. Despite ongoing guidance and regulatory efforts at a national and pan-European level, corporate customers and financial institutions serving them across Europe are still faced with a multitude of country-specific KYC requirements, which hinder both partners from introducing uniform and efficient, let alone digital, KYC processes throughout Europe. The existing fragmentation prevents corporate customers from providing one consistent set of KYC data and supporting documents to their European banking partners, and multinational banking groups from managing AML and CFT risks through aligned and efficient digital EU/EEA-wide KYC processes. This fragmentation comes with high costs and many lost opportunities, both for the bank, which cannot efficiently automate or standardise its controls, and for the corporate, which is faced with additional and time-consuming KYC

requirements, when it wants to expand its business activities across the EU or diversify its banking relationships internationally.

Best practices and specific regulations also dictate that banks must reconfirm all customer data on an ongoing basis. This imposes a significant burden of cost and effort on each institution, which can only be recovered through profitable (corporate) customer accounts – potentially increasing direct or indirect account management charges. To address this problem without reducing the resilience and quality of AML controls, financial institutions must be able to automate certain elements of the KYC due diligence process and limit the assignment of human experts to higher- or high-risk due diligence situations, which require deeper scrutiny and manual risk assessment. This can only be achieved if automated KYC data verification and monitoring processes can be applied consistently, both to domestic and pan-European customer relationships.

### Bridging fragmentation with a KYC Taxonomy for low-risk situations

In early 2021, the Euro Banking Association (EBA) invited its member institutions to assist in the creation of a KYC Expert Group (KYCEG). The core objective of this group of KYC experts was to identify pan-European misalignments in respect to KYC data requirements and any obstacles that hinder or restrict the introduction of cost-efficient automated KYC data collection and monitoring processes. The key questions that the group was trying to answer were how to standardise KYC data collection and how to improve or change the current approach to ensure that these data could be verified continuously and efficiently going forward. →

To find answers to these questions, the KYCEG conducted a detailed analysis of pan-European KYC data requirements and the relative importance of each data point used in the KYC risk assessment process. Upon completion, the KYCEG recommended the publication of a Common Baseline Classification Standard (CBCS) by the EBA in January 2022. According to the experts, the CBCS includes all data points that are relevant to identify and effectively managing AML low-risk corporate relationships anywhere in Europe. If adopted as a standard, the CBCS would enable low-risk corporate customers to create a single KYC information file, which would be suitable input for all its European banking partners and thus significantly improve the efficiency of the KYC process for corporates as customers.

### Other roadblocks are identified but still need to be tackled

During the second phase of the analytical process, the KYCEG identified areas in the KYC data verification and monitoring process in which more alignment and harmonisation at a pan-European level could lead to significant process improvements and cost savings for all parties involved.

At present, significant operational deficiencies are caused by the lack of a harmonised European approach to identifying the ultimate beneficial owner (UBO) of a corporate customer, and the current severe limitations faced by financial institutions or data service providers when they require access to commercial business registers and/or UBO transparency registers to verify corporate customer data. Today, KYC analysts who need to verify client data against official commercial registers are faced with language barriers when accessing some foreign registers that still do not offer an English language service. Registration requirements differ between countries, regional access restrictions may apply, and paywalls restrict access to legally required data. Despite all attempts to harmonise the setup, access to and content of official registers across Europe, financial institutions are not able at this stage to access some registers located

in another EU member state. If language, content, and access to official registers are not harmonised across the European market, the data verification process will remain a highly manual process, and hence costly and inefficient.

Furthermore, there is also no consistent EU-wide approach to encourage official registers to provide open-data files or any other type of machine-readable data to institutions that have to consistently monitor corporate customer data for changes, even between periodic KYC review dates. These misalignments and limitations not only invite systemic risks but also increase the cost of regulatory compliance and hinder the evolution from static-date-driven (periodic) KYC towards far superior risk-based trigger-event-driven (perpetual) KYC processes.

The analysis of the KYCEG and its findings and recommendations have been summarised in the recent EBA publication 'Data Verification for corporate-to-bank KYC in low-risk situations'. Some of the recommendations, for example, the acceptable age of a document used during the KYC due diligence process, will require regulatory adjustments by some EU countries to align with the rest of the EU. Others require goodwill by official registers to align data structures and access mechanisms across Europe. For example, the KYCEG recommends the introduction of a harmonised EU-wide access mechanism that would enable financial institutions to access any official register, ideally through an interconnected portal, without any additional registration requirements at a national level.



[abe-eba.eu](http://abe-eba.eu)

The **Euro Banking Association (EBA)** is a practitioners' body for banks and other service providers. We foster dialogue and experience exchange amongst payments industry practitioners towards a pan-European vision for payments. The EBA has over 160 members from the European Union and across the world.

Follow us on [LinkedIn](#), [Twitter](#) and [YouTube](#).



# The RegTech Association

## North American Regtech Trends



**Deborah Young** is the founding CEO of the RegTech Association. She is passionate about building a community that accelerates the deployment of technology that drives productivity and superior consumer outcomes.

**Deborah Young** ▪ CEO ▪ The RegTech Association



**Alex Ford** is a Non-Exec Director of The RegTech Association and President of Encompass Corporation, North America. She partners with global FIs automating KYC.

**Alex Ford** ▪ President, North America ▪ Encompass Corporation

Regtech is a fast-growing industry, housing rapidly evolving technology solutions that help businesses comply with regulatory requirements. Some estimate the global regtech market size **to reach USD 55.28 billion by 2025**.

The US and Canada are key players in the global market, with many companies, institutions, and regulatory bodies working to harness innovation and shape the industry. At its core, regtech increases the productivity and effectiveness of activities undertaken by regulated organisations. Ultimately, less money is spent on fines and unproductive manual compliance, while businesses move closer to the intent behind regulations.

### Key regulators in North America

One of the things that differentiates North America in most domains is scale – and regulation is no different. With 50 states in the US alone, the number of regulators is vast. AI regtech company 4CRisk.ai notes the US Congress enacts four to six million words of new laws in each two-year congress. Numerous agencies specifically oversee financial institutions and markets – including the Consumer Finance Protection Bureau (CFPB), Financial Crimes Enforcement Network (FinCEN), and the Federal Reserve Board (FRB) in the US and Office of the Superintendent of Financial Institutions (OSFI),

and the Financial Consumer Agency of Canada (FCAC) to name just a few.

### Innovation by regulators

As regtech has become more widely used, proving compliance and operational benefits, regulators have been forward-looking, anticipating its increasing importance. In the recent **Industry Perspectives Report 2022** by The RegTech Association, 44% of regulators indicated regtech/suptech as key priorities, with 44% also planning to adopt in the future and 22% already onboarding solutions.

This has led to various agencies establishing programs such as FinCEN Innovation Hours, the Financial Industry Regulatory Authority (FINRA)'s Innovation Outreach, New York State Department of Financial Services DFS Exchange or the Payment Canada Summit, to encourage a deeper understanding of the industry's solutions, and engagement between regulators themselves and providers. The RegTech Association's global regtech showcase programs have been well supported by regulators including at the recent RegTech Edge No Borders event in New York late in 2022 and their global digital engagement offerings which have attracted 16,000 people from 85 countries since 2020. →

## Use cases and technologies deployed in North American regtech solutions

As in all walks of life, Artificial Intelligence (AI), machine learning (ML), and data analytics have emerged as powerful technologies among the innovative regtech use cases including:

- 1. Risk assessment:** AI algorithms are used to analyse large amounts of data from various sources to identify potential risks in a company's operations. ML models learn from data, better predicting risk.
- 2. Regulatory change monitoring:** The **4CRisk.ai** AI-driven regtech platform offers search capability and horizon scanners to discover new changes to compliance data. The firm aims to significantly lower the cost of compliance and the burden placed on compliance teams.
- 3. Communications security and compliance:** **Theta Lake's** regtech solution utilises machine and deep learning, natural language processing (NLP), and enhanced user experience to capture, archive, detect, and surface risks across video, visual, voice, chat, document, and email content. Capturing and archiving data helps ensure communications are secure and compliant.
- 4. Anti-Money Laundering (AML):** AI and machine learning can increase accuracy when it comes to monitoring transactions, network analysis, and detecting suspicious activities.
- 5. Know Your Customer (KYC):** regtech firm **Encompass** uses automation to eliminate the traditionally manual tasks in KYC due diligence, evidencing the ownership structures of commercial and investment banking customers in minutes.
- 6. Compliance reporting:** AI and ML can automate compliance and regulatory reporting, making it easier for companies to comply with regulations and deliver real-time insights.

Compliance can sometimes lag other areas of the business when it comes to investing in technology and process improvement. The business case for cost containment and improved regulatory outcomes losing out when pitched against growth opportunities. As a result, there is still a heavy reliance on manual procedures, which are costly and inefficient.

The recent bout of activity in the wake of SVB and Signature Bank closures in the US left many banks scrambling to staff their onboarding teams as streams of new customers looked to open new primary accounts or backup facilities. In this context, regtech also has an important role to play in enabling business growth and ensuring continued compliance through automated processes.

## Investment and regtech growth in complex times

While regtechs in EMEA may outnumber those in the Americas (48%: 35%), the level of investment tells a different story. Data compiled by the Boston Consulting Group's FinTech Control Tower (FCT) reports that, between 2000 and H1 2022, investors put USD 13.1 billion of equity investment into regtechs based in the Americas, representing 69% of investment globally.

Since that time, the technology industry overall has entered a different season as faced with layoffs and inflation, the 'top-line growth at all costs' mentality has shifted. The Industry Perspectives report indicated revenue and jobs growth and an increase in capital inflows to the industry from 2021-2022 suggesting that despite the global economic downturn regtech is well placed to weather this climate. Regulations are ever-present and solutions that offer increased efficiencies and sustainable alternatives to human cost-centred reactive tactics will help organisations ensure their house is in order ahead of the next waves of growth.

Undoubtedly, regtech has a critical role to play in society, from helping combat financial crime to improving consumer protection and data rights to boosting operational efficiencies and powering long-term business growth. Going forward, its place and worth will only increase as more businesses turn to regtech solutions and digital transformation initiatives to change the way financial services organisations operate at scale.



[regtech.org.au](https://regtech.org.au)

**RegTech Association**, founded in 2017, aims to promote RegTech innovation and investment to support ethical and compliant businesses globally. The non-profit brings together government, regulators, regulated entities, professional services, and founder-led RegTech companies to collaborate and accelerate the adoption of RegTech solutions in the industry ecosystem.



# Tookitaki

By promoting a collaborative, community-based approach to prevention, Abhishek Chatterjee reveals how Tookitaki's two innovative platforms i.e., AFC Ecosystem and AMLS are revolutionising the fight against fincrime.



**Abhishek Chatterjee** is the Founder and CEO of Tookitaki, a regtech specialising in regulatory compliance through technology and a community-based approach. He earlier worked with JP Morgan, DoubleClick and holds a master's in Applied Mathematics from the University of Southern California.

Abhishek Chatterjee ▪ Founder and CEO ▪ Tookitaki

## What trends have you spotted permeating the financial crime landscape in South-East Asia in the last 12 months?

In the past 12 months, the financial crime landscape in Southeast Asia has seen a surge in digital payment fraud, cybercrime, and cross-border money laundering. Criminals are exploiting gaps in regulatory frameworks and leveraging technological advances to conduct illicit activities. This situation is further exacerbated by the rapid digital transformation brought on by the COVID-19 pandemic, which has led to a greater reliance on online financial services and thus, has increased vulnerabilities. As a result, authorities in Southeast Asia are ramping up their efforts to strengthen regulatory compliance, enhance law enforcement capabilities, and foster cross-border collaboration to combat financial crime effectively. These trends highlight the need for more effective, collaborative, and technologically advanced solutions in the fight against financial crime.

“Tookitaki is paving the way for a safer and more secure financial landscape, by leveraging advanced technologies, fostering collaboration among stakeholders, and addressing the challenges faced by companies.”

## Please tell us more about the Anti-Financial Crime (AFC) Ecosystem in terms of its work, participants, success stories, and challenges.

With criminals employing increasingly sophisticated methods to launder money and evade detection, traditional anti-money laundering (AML) solutions have struggled to keep up. This has necessitated innovative approaches to financial crime prevention.

Tookitaki has developed a unique, community-based approach to financial crime prevention through its two distinct platforms – AFC Ecosystem and Anti-Money Laundering Suite (AMLS).

The AFC Ecosystem serves as a platform for information sharing and collaboration among financial institutions, regulatory bodies, and risk consultants. It facilitates the sharing of best practices, experiences, and knowledge in the battle against financial crime. Its Typology Repository, a living database of money laundering techniques and schemes, is enriched by the collective expertise of its participants. This collaborative platform allows the AFC Ecosystem to adapt and respond to emerging trends and challenges in financial crime prevention.

The AFC Ecosystem has now become one of the biggest communities in the world fighting financial crime. Its members collaborate with each other and share thoughts on the regulatory and implementation aspects of Anti-Money Laundering (AML) compliance. This collaboration has helped create the biggest database of financial crime typologies which is actively being used by AFC Ecosystem members to create more robust AML programmes. →

## What are the biggest challenges currently facing companies in implementing effective AML and fincrime compliance? How is AFC Ecosystem contributing to solving these challenges?

Companies face several challenges in implementing effective AML and fincrime compliance, including fragmented regulatory frameworks, evolving criminal methodologies, and the need to balance customer experience with compliance:

- **Fragmented regulatory frameworks:** companies often need to navigate a complex landscape of laws, regulations, and guidelines across different jurisdictions when implementing AML and fincrime compliance. Regulatory frameworks are subject to ad-hoc changes, requiring companies to stay up-to-date and adapt their compliance efforts accordingly.
- **Evolving criminal methodologies:** financial criminals are continuously evolving and developing new tactics and techniques to evade detection and exploit vulnerabilities in financial systems.
- **Balancing customer experience with compliance:** companies face the challenge of striking the right balance between providing efficient and user-friendly service while ensuring they meet regulatory obligations.

The AFC Ecosystem contributes to solving these challenges by fostering collaboration, promoting knowledge sharing, and providing access to advanced tools and resources. This helps companies in building future-proof compliance programmes that can quickly adapt to changing regulatory requirements across jurisdictions. Companies are also able to identify and mitigate emerging threats without sacrificing the speed and convenience of their services.

## How can companies find the right balance between customer experience and compliance to prevent crime?

Implementing robust AML and fincrime compliance measures often involves additional checks and procedures that can slow down transactions or cause inconvenience for customers. Companies can find the right balance between customer experience and compliance

by leveraging innovative technologies, such as AI and machine learning, to streamline compliance processes while maintaining a customer-centric approach. Tookitaki's two platforms i.e., AMLS and AFC Ecosystem allow companies to enhance detection accuracy and reduce false alerts, improving both customer experience and compliance effectiveness.

## How can firms ensure automated solutions they employ, such as AI and ML, are explainable, and where does accountability lie?

Companies must ensure that their automated solutions are explainable and transparent to maintain trust and accountability. Tookitaki's AMLS uses a glass-box machine learning approach with the explainable AI (XAI) framework, which provides an in-depth rationale for predictions. This approach ensures that AI and ML solutions employed by companies remain explainable, transparent, and accountable.

## Is there a significant disconnect between regulatory bodies and firms? If so, how do we bridge that to tackle financial crime more effectively?

There is often a disconnect between regulatory bodies and firms, hindering the effective fight against financial crime. To bridge this gap, Tookitaki's AFC Ecosystem promotes collaboration and communication between all stakeholders, fostering a united front against financial crime and ensuring that regulatory frameworks and industry practices evolve in tandem.



[tookitaki.com](https://www.tookitaki.com)

**Tookitaki** is a leader in fincrime prevention, dedicated to building a safer world through innovative technology and a community-based approach. It is on a mission to transform the battle against fincrime by dismantling siloed AML approaches and uniting the community through its two platforms – Anti-Financial Crime Ecosystem and Anti-Money Laundering Suite.

# Building Successful and Efficient AML Programs for Today's Business Environment



*The current chilly economic climate will only push more people toward illegal activities. Working together, we can stop the upward trends and even reverse them. Working together, we can all become financial crime fighters.*

**Sandy Lavorel, Financial Crime Fighter, NetGuardians**

# NICE Actimize

## Transaction Monitoring in 2023: Changing the Status Quo



**Ted Sausen**, CAMS, is an AML SME at NICE Actimize. He has 25+ years of experience implementing global enterprise solutions. Before Actimize, he was an SVP at a large financial institution and led the Global Compliance Analytics and Technology group.

Ted Sausen ▪ AML SME ▪ NICE Actimize

When it comes to monitoring transactions for money laundering and financial crime risk, the devil is in the details. Regulations require financial institutions to implement an extensive anti-money laundering (AML) programme, including suspicious activity monitoring. But who decides what is considered suspicious? And how can financial institutions ensure they are mitigating their risks?

Financial institutions have historically taken a broad remit, positioning themselves to address ongoing tech limitations and changes in regulatory guidance. However, this approach has resulted in false positives, overwhelmed AML teams, and provided near-zero visibility into unknown risks.

What's the solution? Anti-financial crime professionals must transform how they monitor and detect money laundering and put a laser focus on making effectiveness a top priority. And the good news is evolution is relatively straightforward.

We don't need to accept the repercussions of an aggressive approach to maximise efficiency and effectiveness. The industry landscape has evolved. AML teams can reset their performance expectations beyond compliance to focus on the truly suspicious activity instead.

### The technology underpinning the evolution of transaction monitoring

The latest advances are crucial to establishing a transaction monitoring (TM) system fit for purpose in 2023. How can an AML programme created years before Teslas, iPhones, and ChatGPT combat sophisticated financial crime today? It can't. Fortunately, TM technology has come a long way since then, as has regulator acceptance of these technologies.

Thanks to recent innovations, FIs can take an entity-centric approach to understanding and monitoring customer risks. By cultivating a holistic understanding of each entity and its network, FIs can detect previously undetectable suspicious activity and turbocharge alert quality.

### The future of transaction monitoring

#### Expanding the role of rules

Technologies like AI and machine learning are head-turners when it comes to detecting more suspicious activity, but they're not infallible. It's paramount that organisations use advanced analytics to complement existing rules-based detection instead of replacing it. Why? Because rules check AI biases, ensuring complete coverage of all known typologies. →

Rules can also enrich machine learning development as engineered features, providing more robust detection and explainability. Organisations must be able to address new threats quickly – rules can instantaneously meet that need, often outweighing the development and training time needed for new machine learning models.

### Connections never before made, found

AML teams' understanding of their customer will become increasingly comprehensive over the next five years. State-of-the-art data enrichment, entity resolution, and network analytics capabilities can settle duplicate records, resolve message counterparties, enrich profiles with relevant third-party risk information, and identify non-explicit entity relationships. This comprehensive understanding will allow institutions to dig deeper into indirect and hidden risks and extend coverage to detect complex or previously unseen money laundering typologies.

### Cross-FI AML collaboration

While privacy concerns can hinder data sharing, without collective industry insights into financial crime, emerging threats, and typologies, the most competent criminals will always find ways to gain the upper hand. Technology will unlock privacy-safe collaboration where other programmes fall short, breaking down industry silos and skyrocketing the prevalence of federated learning, suspicious entity sharing, and cross-industry networks.

### Focus on continuous optimisation

Effectiveness doesn't stop after detection. As organisations adopt advanced analytics to zero in on suspicious activity, feedback after investigations will become pivotal. With this intelligence, machine learning, and simulation teams can refine detection models and customer segmentation, lowering false-positive rates. Teams can also use historical data to minimise manual work and investigation times by shaping workflow, alert escalation, and alert hibernation procedures.

## The beginnings of organisational change

It's inevitable: the evolution of transaction monitoring will change the face of compliance organisations. Advancements in technology will streamline the alerting process. As a result, there will be less demand for junior-level investigators involved in triaging the alerts. Solutions will auto-close many false positives that these investigators are addressing today. And in other cases, they no longer generate these alerts.

The introduction of new analytics will increase the number of true positives. The analytics will identify schemes that current methods are not flagging today. The complexity of these alerts will increase, driving the demand for more senior-level investigators.

However, no technological innovation comes without a cost. They're complex. They require knowledgeable resources and data science experts. AML know-how will prove to be essential to implementing current technologies effectively. As a result, compliance organisations will begin to create new technology functions dedicated to their organisation.

On the other hand, less is more. As technologies shift to the cloud, fewer compliance-focused IT individuals will be needed to maintain technology infrastructure. Solutions providers will start carrying that expertise in place of FIs.

## Moving beyond the status quo

We're at a turning point in transaction monitoring. We have all the tools needed to detect money laundering more accurately and focus on genuinely suspicious activity. It's time to stop chasing false positives in the name of compliance and fight financial crime!

If you'd like to find out more about the future of transaction monitoring and how technology can drastically improve your transaction monitoring detection, check out this [video](#) or contact [NICE Actimize](#) today.

[Click here for the company profile](#)

**NICE Actimize**

[niceactimize.com](https://www.niceactimize.com)

**NICE Actimize** is the largest provider of financial crime, risk, and compliance solutions for financial institutions. The company offers real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance products that address payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence, and insider trading. Find us at [www.niceactimize.com](https://www.niceactimize.com)

# Feedzai

Money mules constitute both a fraudulent and a money laundering problem, it requires a holistic solution rather than being viewed solely as a compliance concern for a particular regulation.



**Mike Nathan**, with 15+ years in risk and fraud, specialises in online banking, application, internal fraud, money mules, anti-money laundering, and card fraud. He's held management positions at Lehman Brothers, Lloyds, SAS, Barclaycard, and LexisNexis, and now leads a team at Feedzai, advising top financial organisations.

Mike Nathan ▪ Global Head of Solutions Consulting ▪ Feedzai

## What are the challenges in fighting money laundering?

Money laundering involves two distinct aspects – compliance and the prevention of illicit funds movement in the financial system. Compliance is crucial for banks to avoid fines and regulatory scrutiny, but identifying and preventing money laundering requires going beyond compliance.

Addressing money laundering and fraud is challenging because certain (positive) activities can be easily manipulated for fraudulent purposes. For instance, COVID-related funds created new opportunities for shell companies to be used for fraud and money laundering. This makes money laundering and fraud two sides of the same coin.

“Monitoring banking inbound payments will become an essential cog in preventing fraud and money laundering.”

In the banking industry, the identification of money mules is tackled differently depending on the bank. For instance, in the case of some banks, it's considered an AML problem, and they have dedicated analytics teams, technology, tools, and investigators all looking at money mules. In other cases, banks are relying on fraud teams to detect money mules and investigate money mules' accounts to reduce their losses.

## What are money mules?

Money mules are accounts that are used to receive illicit funds, whether it's for fraudulent or money laundering purposes. Bad actors use various means to target money mules, such as instant payments/faster payments, internet banking, and transfers. Money mules are necessary for these types of fraud because fraudsters need a way to receive the funds, they are an essential vehicle for fraud. There are two types of money mules: recruited mules and unwitting mules. Recruited mules are paid to open bank accounts and give their details to fraudsters. Unwitting mules are people who unknowingly allow their accounts to be used for fraud. This can happen when someone tricks them into sending money to another account.

The typical profile of a money mule is someone who may be struggling with financial difficulties or is vulnerable to offers that sound too good to be true. While it was previously targeted toward young people, nowadays it can be anyone, especially in times of economic crisis. Fraudsters play a volume game, preying on those who need quick cash. Demographics also play a role, with location and income being factors that can make someone more susceptible to becoming a money mule.

## How do instant payments impact money mule activities?

Instant payments have had a significant impact on the rise of fraud and money mule activities. Banks are investing in technologies such as device identifiers, behaviour biometrics, and more screening tools to risk assess payments. However, with the rise of scams, the vulnerability no longer sits with the bank, it's the customer. →



As a result, scams have become the predominant type of fraud as fraudsters look for ways to bypass the new defences. I remember once, one of the major banks in the UK said to me that ‘if you find all the mules, you can stop all the fraud’. This idea resonated a lot with me, and I have spent a lot of time putting in place strategies to try and prevent money mule accounts from taking place. A further overlap with money laundering is this kind of concept of layering, a foundational element of anti-money laundering where the fraud moves between banks and goes through multiple iterations, second, third, fourth generation mules, washing the money through the system, making it much harder for the banks to identify.

This has led the Payment Services Regulator (PSR) to put forward [proposals around scam reimbursement in the UK](#).

### What mitigation strategies can banks put in place to prevent money mules?

Monitoring banking inbound payments will become an essential cog in preventing fraud and money laundering. The trigger event for a money mule is the inbound payment, this needs to be risk assessed holistically to prevent a further outbound payment, reducing fraud and scam losses, and stopping money mules layering accounts. Another such strategy is to prevent money mules from re-entering the bank’s ecosystem by listing their attributes, such as device IP, and using link analysis and graphs to investigate other shared accounts. However, these strategies are reactive and rely on fraud taking place. The use of Machine Learning can help banks build a predictive model to enable them to anticipate which accounts are likely to be money mules. It is powerful to use a model in conjunction with other strategies; to alert on a large transaction that it scored badly on the model.

It is important not using the model as a raw investigation tool, but to enhance the controls you currently have in place.

In addition to the strategies mentioned earlier, we must consider the human side of things when trying to achieve a holistic view of inbound and outbound transactions. Closing someone’s account or stopping someone from doing their banking due to an incorrectly labelled transaction can be detrimental. Furthermore, fraudsters may use various tactics to obtain accounts, such as offering free trips or other incentives to unsuspecting individuals. It’s crucial to keep in mind that being convicted of being a money mule can have serious consequences, including prison time. Therefore, it’s important to balance the need for effective mitigation strategies with the need to ensure that innocent customers are not unfairly impacted.

[Click here for the company profile](#)



[feedzai.com](https://www.feedzai.com)

**Feedzai** is the world’s first RiskOps platform, protecting people and payments with a comprehensive suite of AI-based solutions designed to stop fraud and financial crime. Feedzai enables leading financial organisations globally to safeguard trillions of dollars of transactions and manage risk while improving their customers’ trust.

# NetGuardians

## Co-operate to Eliminate: a Community Approach to Beating Financial Crime



**Sandy Lavorel**, a NetGuardians financial crime fighter, is a Certified Fraud Examiner and an expert in Anti-Money Laundering. He has several years of consulting experience and is a fervent advocate of the collaborative approach to fighting financial crime.

Sandy Lavorel ■ Financial Crime Fighter ■ NetGuardians

*In a breakthrough in the fight against financial crime, the Swiss fintech has developed a way for banks to share information on fraud risk that not only significantly improves detection rates for fraud but also identifies accounts used for money laundering.*

Banks, regulators, policy-makers, and law enforcement have to date treated fraud and money laundering as two very different, unrelated, difficult-to-prevent crimes. Even the teams within banks and other organisations dealing with fraud and money laundering are often siloed. This is a mistake that criminals easily exploit, as evidenced by the record amounts being lost to fraudsters and laundered worldwide through the banking system.

### The scale of failure

The **FBI** received reports of online scams causing losses exceeding USD 10 billion in 2022, marking the greatest annual loss over the past five years. Further, according to the **United Nations Office on Drugs and Crime**, about 3.6% of global GDP (approximately USD 1.6 trillion) is laundered every year.

Failure on this scale cannot continue, which is why we're calling for banks, regulators, and policy-makers to adopt a new approach. One that acknowledges and takes advantage of the very close links between the two crimes, draws on community intelligence and promotes collaboration and cooperation.

Any money the fraudsters steal must be washed through money-mule bank accounts. If we can identify and confirm a fraudulent transaction, we can identify the destination — or the mule accounts. Using this knowledge allows us to catch the fraudsters and stop the laundering. But it's easier said than done.

### Diverse challenges

The challenges of doing so thus far have been manifold. There's the ever-evolving nature of the fraud scams and methods that make them harder to spot, while the ease and speed at which criminals can open digital bank accounts through which to wash their cash makes them hard to track. There are also data protection and privacy regulations that prevent banks from easily sharing information linked to suspicious accounts, often stopping one bank from warning others.

Unless we do something fast, things are only getting worse.

The current cost of living crisis and harsh economic climate are pushing more people toward crime, ensuring a steady supply of money mules and individuals willing to front scams. This trend is being facilitated and fuelled by dark web sales of software-as-a-service for fraud scams, which means people can commit fraud without having to be computer experts.

Together, these worrying trends make it clear that more effective prevention and detection are a priority. Indeed, banks themselves have already started to call for more cooperation in these areas.

### Compliant data-sharing is key

At a recent international anti-money laundering and fraud conference in London, for example, representatives from banks including ING, Commerzbank, and Lloyds all agreed they need to cooperate more and share data to stop the criminals. But, mindful of the challenges, are unsure where to turn. →

Numerous techniques can be employed to ensure data retains its core intelligence value whilst simultaneously respecting security, confidentiality, and liability concerns. This anonymised data could be shared to protect customers and prevent financial crime.

At **NetGuardians**, that is exactly what we do.

For more than a decade, we've been successfully helping banks worldwide to stop fraud. By drawing on this success, and our understanding that where there's a fraud attempt there's also a money mule, we've developed a service that is proving powerful in the fight against both.

Our **Community Scoring & Intelligence Service (CS&I)** pools anonymised transaction data from participating banks to gain more insights. It aggregates the data we receive, cleans it, standardises, and formats it so that the resulting intelligence is easy to understand and can be used immediately by member banks to enhance their analytics and help them more accurately assess the fraud risk of every transaction.

In addition, the service also focuses on the receiving account to spot money mules.

Whenever we spot fraud, we know that the receiving bank account will be the start of a money-mule journey. The anonymised data that banks share with us enables us to identify the receiving mule account. We share this intelligence compliantly with other banks, including the receiving bank, to alert them.

### Community effort

The more banks that participate in the community, the more information there is about both fraudulent activity and money-mule accounts. We believe that by adding in further intelligence from carefully chosen third parties such as law enforcement agencies, we will be able to prevent far more fraud and identify and stop money mules. As more banks join, we create a virtuous circle.

Banks already using our software see the opportunity to tackle fraud and money laundering simultaneously. They are reaping the benefits and are eager for others to join. As the head of risk at one private bank client says: 'We can stop money mules if we co-operate. It's time to share data across institutions to prevent these crimes and, where we can't prevent them, to recover the assets.'

Our service could not come at a better time. The current chilly economic climate will only push more people toward illegal activities, including becoming mules for money launderers and perpetuating frauds themselves. Working together, we can stop the upward trends and even reverse them. Working together, we can all become financial crime fighters.

[Click here for the company profile](#)



[netguardians.ch](https://netguardians.ch)

**NetGuardians** helps financial institutions worldwide to fight financial crime. Over 100 banks and wealth managers rely on NetGuardians' 3D artificial intelligence solution to prevent fraudulent payments in real time. NetGuardians partners with major banking software companies, including Finastra, Avaloq, Mambu, and Finacle. Headquartered in Switzerland, it has offices in Singapore, Kenya, and Poland.

# Huron

## Integrating AI/ML/NLP for Financial Crime Compliance: Analysing Technical Complexities and Customised Implementations



With 20+ years of compliance and anti-financial crime experience, **Alan** specialises in strategic planning, technology integration, risk mitigation, and change management. His expertise spans US, Canadian, UK, and APA financial regulations, and he has held leadership positions at JP Morgan/Bear Stearns, Adsideo LLC, Oliver Wyman, and Sapient.

**Alan Morley** ■ *Director, Anti Financial Crimes and BSA Advisory* ■ Huron



With 20+ years of experience, **Fanny** drives business transformation, customer experience, and automation maturity for institutions across multiple industries. Her expertise spans consumer products, higher education, energy, financial services, and healthcare. Fanny previously held leadership positions at UiPath, McKinsey & Company, PwC, and Deloitte.

**Fanny Ip** ■ *Managing Director* ■ Huron

In recent years, the banking industry has increasingly relied on artificial intelligence (AI) and machine learning (ML) techniques to combat fraud and money laundering. These techniques, when combined with natural language processing (NLP), can provide banks with powerful tools for detecting and preventing illegal financial activities. However, there are significant challenges to implementing these technologies effectively.

One of the main challenges of AI and ML in banking fraud detection is the need for large and diverse datasets. To train models to accurately identify fraudulent activities, banks must have access to data from a wide range of sources and transactions. This data can be difficult to obtain, particularly for smaller banks or those with limited resources.

Another challenge is the complexity of financial transactions. Money laundering and fraud can take many forms, and it can be difficult for even the most sophisticated machine-learning models to detect all of them. Additionally, fraudsters are constantly evolving their tactics, which means that models must be continuously updated and refined to stay effective.

The implementation of these technologies also requires significant investment in IT infrastructure and expertise. Banks must have the resources to develop and maintain the necessary software, hardware, and data storage systems. They also need to employ data scientists and AI experts who can work with the technologies and ensure they are used optimally tuned.

In addition to these technical challenges, there are also legal and ethical considerations to consider. Banks must ensure they are complying with relevant regulations, such as the General Data Protection Regulation (GDPR) and the Bank Secrecy Act (BSA). They must also be transparent with customers about how their data is being used and ensure that the technologies they use do not perpetuate biases or discriminate against certain groups.

Despite these challenges, AI, ML, and NLP are increasingly being used in banking fraud and anti-money laundering detection, with the potential to significantly improve banks' countermeasures and to ensure the integrity of the financial system. However, it will be essential for banks to invest in the necessary resources and expertise to implement these technologies effectively and responsibly. →

Several potential issues can arise when implementing AI, ML, and NLP technologies. Some of the most significant include:

- 1. Biases and discrimination:** one of the biggest challenges with AI, ML, and NLP is the risk of biases and discrimination. These technologies are only as good as the data they are trained on, and if that data is biased or incomplete, it can lead to inaccurate or unfair results. For example, if a system is trained on data that reflects historical biases against certain groups, it may perpetuate those biases when making decisions.
- 2. Lack of transparency:** AI, ML, and NLP models can be complex and difficult to understand, which can make it hard to explain how decisions are being made. This lack of transparency can be a concern in industries like finance, where customers may want to know how decisions about their money are being made.
- 3. Overreliance on technology:** it's important to remember that AI, ML, and NLP are just tools, and they should not replace human judgment entirely. Overreliance on technology can lead to a lack of critical thinking or oversight, which can cause problems down the line.
- 4. Data privacy and security:** AI, ML, and NLP require access to large amounts of data, which can be a potential target for hackers or other bad actors. It's important to ensure that appropriate security measures are in place to protect sensitive data.
- 5. Lack of standardisation:** there are many different AI, ML, and NLP tools and techniques, and they are not always standardised or interoperable. This can make it difficult to integrate different systems or compare results across different models.
- 6. Technical skills requirements:** AI, ML, and NLP are complex technologies that require significant expertise to develop and maintain. Implementing these technologies can require significant investments in IT infrastructure and talent and may not be feasible for smaller organisations.

#### **7. The gap between data scientists and front-end operators**

(developing a positive feedback loop): data scientists usually develop and train the ML model based on initial requirements. After they deploy the ML model, there is no formal cadence to update it. On the other hand, the masterminds of financial crimes keep evolving. Front-end operators are, fortunately, often up to date on the new tactics, but there is often no feedback loop between these operators and data scientists that would make the ML model relevant and effective.

#### **8. Preparing the System:**

training both parties on how to apply real-world activities in such a way as to help the ML models learn effectively and quickly will boost the cost-to-performance ratio. Learning activities include breaking down a use case into steps, identifying the critical data elements and expressing how each piece of data is used (or generated) by the bad actor will better inform the system as it evolves. This takes practice.

For example, when looking at payment activities over a long period, each segment, or group, will exhibit a series of behavioural oscillations as repeat payment types, amounts, and frequencies involving third parties develop a 'moving average' of sorts. Interestingly, it is the customers who never oscillate, whose behaviours run counter to the group norm and who seem too quiet are often too quiet for a reason. Teaching the ML model to look for the inverted anomaly can quickly reveal suspicious behaviours that have been flying under the radar for a long period. Not all bad actors behave outside the standard deviation of the group norm, sometimes they are too close to the mean for way too long.

Lastly, it's important to approach the implementation of AI, ML, and NLP technologies with a critical eye and a focus on transparency, fairness, and accountability. By doing so, it is possible to harness the power of these technologies while minimising potential risks and drawbacks while optimising the expected return on investment.

**Huron** is a global professional services firm that collaborates with clients to put possible into practice by creating sound strategies, optimising operations, accelerating digital transformation, and empowering businesses and their people to own their future. By embracing diverse perspectives, encouraging new ideas, and challenging the status quo, we create sustainable results. For more information see [huronconsultinggroup.com](https://www.huronconsultinggroup.com)

# NatWest Group

## How to Strike the Perfect Balance Between Computer-Led and Human-Led Transaction Monitoring for Maximum Efficiency and Effectiveness



**Colin Whitmore** is an AML subject matter expert, he brings over 20 years of experience within the banking and financial services, working in the UK and the US with firms including Reuters, Aviva, Barclays, RBS, HSBC, and now the NatWest Group.

Colin Whitmore ▪ *Head of TM Strategy, Innovation and Design* ▪ NatWest Group

TM has served as a backbone of efforts to detect and prevent money laundering within financial services and other sectors. In many cases, the production of alerts has been an automated approach, often using a rule-based application. People are employed to 'work' alerts, which usually involves information gathering, reviewing transactions, and understanding the rationale for customer behaviour. Based on this alert working, and subsequent investigation a SAR 'Suspicious activity report' may be disclosed to the relevant law enforcement.

This process has worked, and continues to work, in a fashion that is expensive and time-consuming, with humans performing many 'routine' tasks such as information gathering, before decision making. It is not cheap and with many alerts being closed out, it can be a demotivating activity for the humans in the loop, who spend a lot of time looking at nonvalue alerts.

Unfortunately, compliance can be seen as a break in growth, often having a significant cost, both in terms of the systems management and the number of people required in the operations. Firms have to manage the cost and effort, remain within the law and continually review their systems and approach. The costs and limitations of monitoring, in terms of new products, or threat responses can prevent firms from expanding into new markets or releasing new products for fear of overwhelming their AML operations or failing out of compliance.

This is where the balance comes in. Currently, the process is highly people-intensive, and arguably the wrong type of people-intensive, as noted previously a significant amount of time and effort is spent

gathering information, performing online searches, and documenting outcomes as opposed to making decisions.

Firms know the issues, but to date have had little room for manoeuvre, on the systems side improvements have been incremental, not evolutionary. On the people side, they have a focus on employing and retaining more and more people. So, I hear you ask, what can be done in this situation? How can firms expand their compliance coverage, making it more effective, without the overwhelming costs? What is the vision? Where are firms heading and what is the future for TM?

Fortunately, we are now at a point where innovative and new approaches, focused on data, analytics, networks, and intelligence can start to turn the dial, moving TM away from 'producing and clearing alerts' to intelligence lead financial crime investigations. Here are some simple steps that firms could consider to address the balance.

- 1. Set a vision and strategy, with a roadmap** – Where do you want to be, what is the vision, what do intelligence lead detection and investigations mean? How can you use data and analytics, what does it mean for your current operations and employees, and what new skills will they need to have? How can you achieve this, over a 12-24-, 3- and 5-year time scale? Take time to document, socialise, and agree, even if it looks currently unattainable. →



**2. Automate routine activities** – What are the immediate gains you can make, at lower cost, which bring quicker benefits? In particular, the automation of routine activities such as information searching and gathering, documenting, and preparing information for decision-making. With tried and trusted technologies such as RPA, NLP, and NLG this is very achievable.

**3. Refine current output** – How can you refine the output from current TM systems, the application of scoring and prioritising, after the production of ‘events’? Usually, this is based on data enrichment, the use of analytical and statistical models, and supervised learning, as an example, based on human outcomes on similar events. There are several choices here, including what you use to score, what additional data you use for discounting, enhancement, and what you do with the output, do you hibernate, or do you close?

**4. Produce less noise** – focus on quality, reduce the number of alerts produced in the first place, reducing the ‘noise’ when compared to ‘signal’. A word of warning here, this is not a focus on ‘false positive’ reduction to the detriment of other controls, it is not a comparison of ‘x% versus Y%’ but a careful and thoughtful use of good data, customer segmentation, and augmentation of new innovative approaches.

**5. Augment with innovative approaches** – there are many new approaches and solutions, can you start to trial and use some of these solutions across the entire operation or for specific business areas and threats? What is already in use in the industry? Are you replacing or augmenting current systems? How can you trial and test before going to full use, what does it mean for operations?

**6. Move to intelligent lead investigations** – by reducing noise, augmenting current approaches, and using enhanced, and shared data and analytics to support well-trained human decision-makers, you can move towards intelligent lead investigations. This will need to be defined for your firm, what are the journey and roadmap?

In summary – the balance between computer-led and human-led transaction monitoring does not currently support an effective and efficient TM function. Doing more of the same will not enable firms to make the step change in how they approach Transaction monitoring.

However, firms can start to take steps toward a new balance, once which is more efficient and repeatable, through the application of intelligence, data, networks, and analytics. Importantly, the need for people will not go away, the ‘human in the loop’ is critical, this is about moving the balance, using technology and analytics sensibly to free up people from the mundane, supporting the intelligence lead detection and prevention of financial crime.



[natwestgroup.com](https://www.natwestgroup.com)

**NatWest Group** is a relationship bank for a digital world. We champion potential; breaking down barriers and building financial confidence so the 19 million people, families, and businesses we serve in communities throughout the UK and Ireland can rebuild and thrive. If our customers succeed, so will we.

# Banking Circle

## From Rules to Models: Improving AML Decision-Making with Machine Learning



**Ruben**, PhD, has a background in engineering and computing with a focus on optimisation and control theory.

Ruben Menke ■ *Lead Data Scientist* ■ Banking Circle



**Robert** has a PhD in computer science and a background in working with data and automation in the banking sector.

Robert Norvill ■ *Senior Data Scientist* ■ Banking Circle



**Christian** has a PhD in engineering and worked across network analytics, optimisation and AI/machine learning.

Christian Karsten ■ *Head of Advanced Analytics* ■ Banking Circle

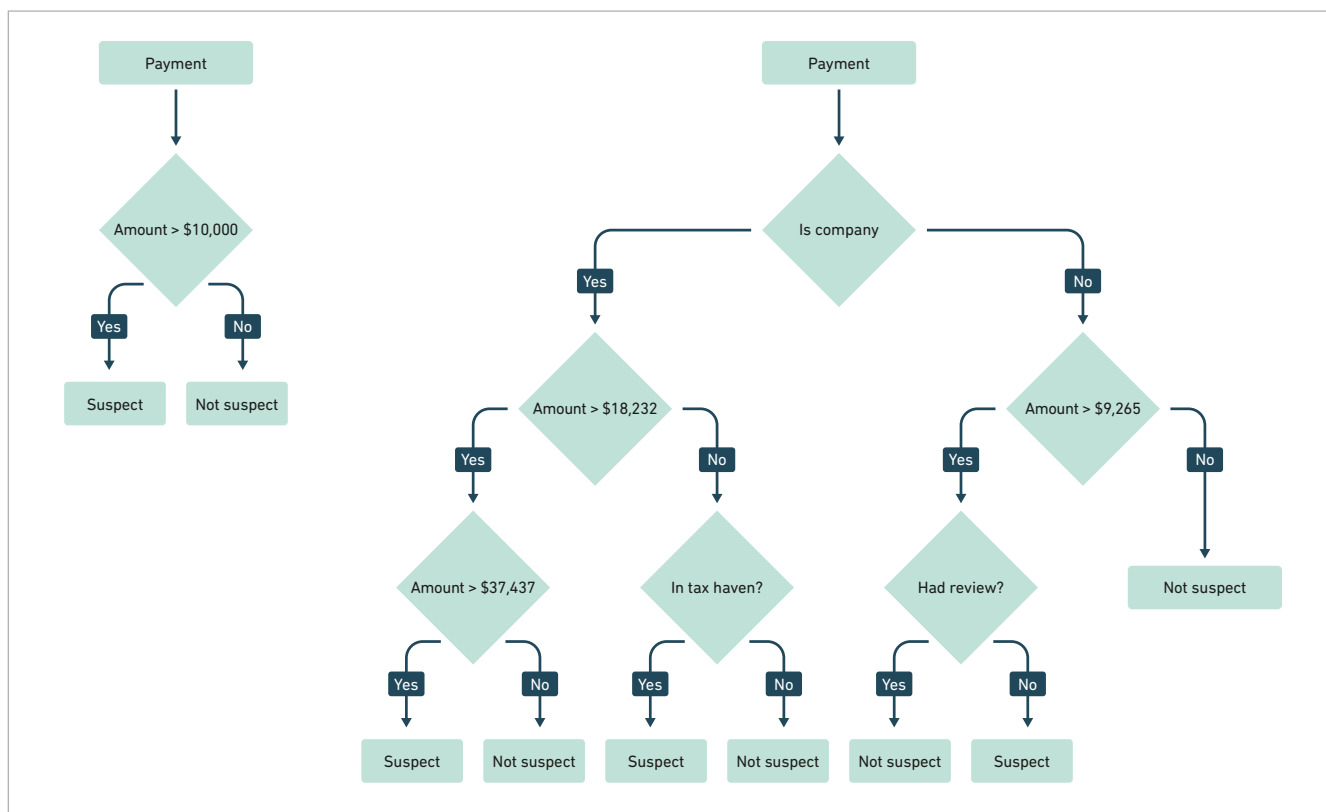
Banks and other financial institutions face thousands of decision problems every day. Some are simple, and decisions can be made quickly and efficiently by a single person or handled through automation. Others are on a different scale and require much more effort to be solved properly. These problems often have a significant bottom-line impact and, in the case of Terrorist Financing (TF) or Money Laundering (ML), also regulatory impact.

Consider, for example, a bank like Banking Circle which has built the first and only real-time clearing and settlement network for 24 currencies to deliver faster, lower-cost payments. The AML team's role is crucial to this mission as they ensure all solutions are fully secure and compliant all the way from onboarding to live TF/ML monitoring of payments.

This requires a more sophisticated and powerful payment screening decision system than the traditional rules-based AML setup where decisions are made on one or two variables such as amount, date, location of the payee, etc.

The problem with a rules-based approach is that, from a machine learning perspective, the rules look a lot like a shallow, badly tuned decision tree (see figure 1). They are most often tuned by hand, and decision points are adjusted using intuition and an understanding of the way things have always been done. This approach generally leads to false positive rates of 97-99%. Rules-based systems are usually improved by adding rules and tweaking where decision points are set. For e.g., what amount and location combination correlates with a higher likelihood of a SAR filing? →

Figure 1: A traditional AML rule (left) vs a simplified representation of a machine learning-based model (right).



Automating the improvement process and using many more variables gathered from a wide range of sources is the essence of machine learning applied to this space. It provides a decision-making method capable of identifying and utilising correlations that are impossible for humans to find and use by hand. We often refer to this set of more complex rules as a model.

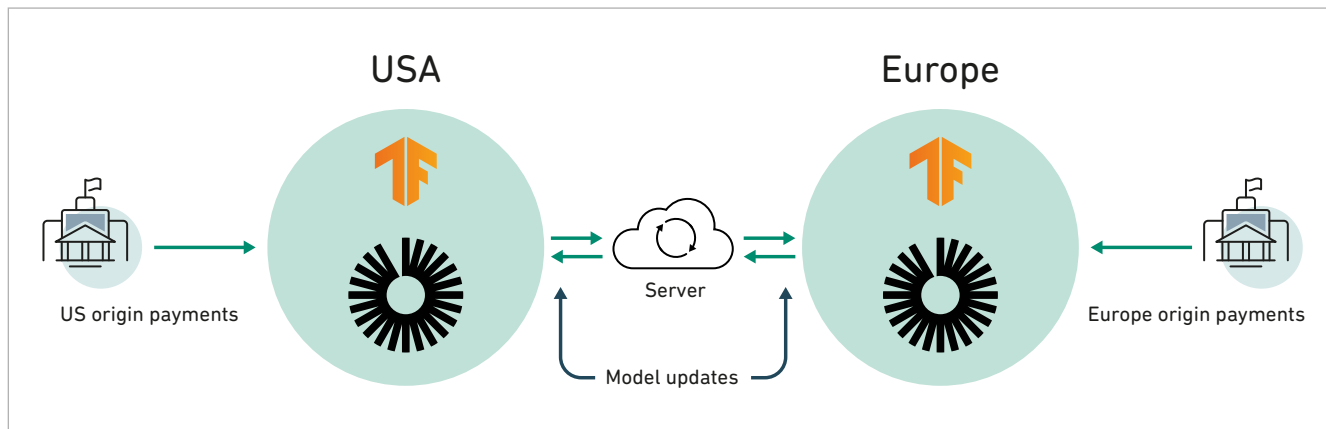
While hand-crafted rules are not completely outdated – they are still useful to filter out very obviously suspect payments – they should be seen as the first step in a modern AML pipeline. A modern system contains multiple machine learning steps and ends with analysts investigating payments. In a world of increasingly sophisticated financial criminals, it becomes not only a value add to utilise the proper machine learning tools, but simply necessary.

Machine learning is trained on historical data and expects the payments evaluated to be similar to the payments of the past. This is also true for rules. However, machine learning models can be improved by diversifying the data they learn from, and diversification models can be used as part of an AML pipeline for this purpose. For example, knowing how different payment is compared to previously analysed payments, or how much a customer’s behaviour (e.g., frequency of payments) has changed over time can improve model performance.

An important consideration when introducing such systems is to evaluate the AML risk. A rules-based system is binary and will not consider or assign any risk for most payments as only a fraction of the total number of payments is flagged and assessed. This hides information about a large part of the flow. Machine learning-based models assign a risk level to all transactions. Not doing this leaves banks unaware of their flow risk. Crucially, a machine learning model finds suspicious flow that a normal rules-based setup cannot. It can reduce false positive rates by 10x or more, automatically adapt to new scenarios and increase detection of true positives, allowing analysts to focus on relevant payments without being flooded with payments they don’t need to see.

Embracing machine learning opens up new opportunities for collaboration within banking and finance that simply do not exist when using traditional rules. Banking Circle has recently developed a federated learning system. Federated learning is when multiple participants contribute to training a model, see Figure 2, without sharing data. →

**Figure 2: Banking Circle's federated learning system.**



Each participant trains using their own local data and shares the findings with a server which uses them to build an improved global model while retaining the knowledge gained from each participant. Only the machine learning updates from each participant are sent to the server, never data. This enables a number of interesting possibilities. For Banking Circle, the internal use case is sharing knowledge to train a model to analyse US payments without exposing European data.

Together with the ability to identify complex flow patterns, utilise more data to discover previously hidden pathologies, and provide an improved understanding of flow risk, it is clear that not using machine learning in AML risks enabling money laundering.

Here, we can train a much more effective US model while remaining fully compliant with data protection laws in Europe. Having one participant in Europe training on EU data, and one in the US training on US data, both contribute to a single federated model that retains the knowledge of both participants. Looking beyond this, when considering the need for machine learning in modern AML and the privacy preservation that federated learning provides, as the opportunity for banks to collaborate in a federated learning system to train a model more performant than any of them could train individually.



[bankingcircle.com](https://bankingcircle.com)

**Banking Circle** is a fully licenced next-generation Payments Bank, designed to meet the global banking and payments needs of payments businesses, banks, and online marketplaces. Banking Circle solutions power the payments propositions of 300 financial institutions across the globe, including 16 banks.

# Key Considerations for Companies Entering the Crypto Market



*Cryptocurrencies are an emerging area of payments and investments, FIs cannot realistically bury their head in the sand and ignore them. At a minimum, they need to put in robust controls to detect and protect, not only for their own safety but that for their customers and wider society.*

**Colin Whitmore, Head of TM Strategy, Innovation and Design, NatWest Group**

# NatWest Group

## Best Practices in Preventing Money Laundering through Cryptocurrency Exchanges and Custodian Services



**Colin Whitmore** is an AML subject matter expert, he brings over 20 years of experience within the banking and financial services, working in the UK and the US with firms including Reuters, Aviva, Barclays, RBS, HSBC, and now the NatWest Group.

Colin Whitmore ▪ *Head of TM Strategy, Innovation and Design* ▪ NatWest Group

Cryptocurrencies are in the news on a daily basis, whether it is in headline-grabbing articles such as the sudden and dramatic failure of crypto firm FTX, or the use of cryptocurrencies in ransomware and other criminal activity. Indeed, if you were to look at sites on the dark web, such as those selling drugs, personal identification information or weapons, you would see that payments are required in cryptocurrencies. Criminals are using cryptocurrency to avoid detection and move their illicit funds from one jurisdiction to another, avoiding sanctions and engaging in fraud and money laundering without detection.

However, to claim that all cryptocurrency is used for criminal purposes would be a mistake. Not only does it disregard legitimate and legal investment, but it is a statement, often made without consideration of poorer regions of the world where the national Fiat currency is unstable, or access to banking services is expensive or limited. Often in these countries, cryptocurrencies provide a means of transferring money or buying goods, often from China, for sale in the local community. Cryptocurrencies can be more stable (especially considering stablecoins) and can provide more surety than other methods of payment.

So where does this leave FIs? How should they approach cryptocurrencies, and importantly manage the risks? Relying on the Virtual Asset Service Providers (VASPs) themselves is not enough. Yes, some VASPs will have controls in place, with established KYC/CDD undertaken on their customers, and the ongoing monitoring of customer activity. However, from a risk perspective, FIs need to understand and manage their risk, for themselves, especially

where cryptocurrency is moved to and from Fiat currencies – the ‘on/off ramps’.

Thankfully, there are several practical steps firms can take, which I will explore:

### 1. Establish a clear risk statement and appetite

A good first step is to understand the environment, where the firm stands, does it want to avoid cryptocurrencies altogether (which is a difficult position to maintain), become a custody provider, or provide banking services to VASPs? The firm needs to decide and document its risk appetite and what this means in terms of controls.

### 2. Build awareness

The firm should look to build awareness across senior management, the compliance function, and wider across the firm, enhancing knowledge of the risks.

### 3. Monitor exposure – including a risk-based view

Even where a firm does not want to provide cryptocurrency services they need to have, at a minimum, an accurate view of their exposure. Through the use of data sets and the understanding of payments, a FI can identify exposure across their customers. An enhancement to identification is the risk rating of the payment activity and exposure. Not all VASPs are the same, and not all transactions have originated from safe sources – this is where specialist providers come in, they provide an understanding of the VASPs from a risk profiling perspective. →



#### 4. Understand a customer's source of funds

There is a risk that firms are accepting wealth generated from illicit cryptocurrency without knowing. Asking the customer if any wealth originates from cryptocurrencies does not really work. Not only are you relying on the goodwill and honesty of the prospective customer, but how can you check? This is where currency tracing comes in, the prospective customer is asked to provide their wallet address from which the firm can then check previous activity. This is similar to asking for the last x months' bank statements or payslips, or evidence of investment gains, share sales or property transactions etc.

#### 5. Complement existing controls

How can enhanced data and intelligence be used to complement existing transaction monitoring, fraud, tax, and sanctions controls? This is a combination of data, intelligence, and enhanced intelligence, with enhancements to existing controls. Going beyond current approaches, new innovative detection based on data analytics is used to identify particular anomalies and patterns specific to cryptocurrencies.

#### 6. Build an investigative capacity

Do not forget the people! How can you enhance the skills and knowledge of your people? Yes, some of this is through awareness, but more to the point what specialist tools and training can you give to your investigators? Fortunately, specialist investigative tools exist, that have been 'honed' through extensive use by law enforcement. These tools allow firms to 'follow the currency' on the chain, and follow the sources and movements of funds. These are not tools for general use within sanctions, transaction monitoring or fraud operations, but enable trained threat intelligence investigators to drill down on the initial leads and follow the crypto chain.

### In Summary

This is a journey for firms. Following incremental steps, they can move towards a position of awareness and robust risk controls. We are now at a point where there are specialist vendors in this space who work daily with FIs, law enforcement, VASPS and other firms to provide data, intelligence, and tools for identifying and controlling financial crime risks.

With documented and robust controls, FIs can decide their approach to cryptocurrencies and the custody of digital assets. Whether that is the desire to avoid cryptocurrencies, custodians, exchange services or the provision of banking products and services to VASPs. Cryptocurrencies are an emerging area of payments and investments, FIs cannot realistically bury their head in the sand and ignore them. At a minimum, they need to put in robust controls to detect and protect, not only for their own safety but that for their customers and wider society. FIs need to consider those who may not have easy access to other forms of finance, this is not about exclusion, but if done thoughtfully and in a controlled manner can lead to greater inclusion.



[natwestgroup.com](https://www.natwestgroup.com)

**NatWest Group** is a relationship bank for a digital world. We champion potential; breaking down barriers and building financial confidence so the 19 million people, families, and businesses we serve in communities throughout the UK and Ireland can rebuild and thrive. If our customers succeed, so will we.

# Nuvei

Nuvei's AML Compliance Officer, Antonia Michail, provides updates on EU's 6th AML directive, and how is impacting FIs and crypto providers.



Nuvei's AML Compliance Officer, **Antonia**, guides and trains global staff on AML and regulatory compliance. With 15 years of financial services experience, she's knowledgeable in VASPs European Regulatory Framework, M&As, and Blockchain, and is certified in CAMS and CySEC's AML. Antonia holds multiple degrees and speaks four languages.

Antonia Michail ▪ AML Compliance Officer ▪ Nuvei

## What are the key changes and updates in AMLD6, and how will these impact financial institutions and other affected entities, especially those operating in the crypto sector?

Let's start by saying that the 6th Anti-Money Laundering (AMLD6) is part of a broader effort of the EU Commission to tackle Money Laundering. The Commission is giving a more dynamic and international character to its approach, by further expanding the definition of money laundering and related predicated offences – now increased to 22 – and including environmental crime, cyber-crime, and certain tax crimes. The directive is also setting stricter punishments for non-compliance for both legal and natural persons and aligns with Financial Action Task Force's (FATF) revised Recommendations and approach towards third countries – as a country being listed by FATF will now also be listed by the EU.

“ Companies operating in the crypto sector will now need to have a proper licence and collect originator and beneficiary information for all their digital assets.

The AMLD6 is also enhancing Financial Intelligence Unit (FIU) coordination and cooperation, which leads to more efficient results. Moreover, we see the introduction of new rules and minimum standards to be followed by domestic supervisors and a more

convergent approach towards these standards via the Anti-Money Laundering Authority (AMLA). AMLA will have a more centralised role in terms of AML/CFT supervision in cooperation with the national authorities.

Compared to its predecessors, the AMLD6 does not require the obliged entities to introduce heavy changes in their AML policies and procedures. However, it should be noted that the term 'property' in the new definition of money laundering now also includes tangible and intangible, electronic or digital, assets, and the conversion or transfer, concealment, and acquisition or possession of such property derived from criminal activity is punishable as a criminal offence.

Additionally, the issue of territoriality is important as this would extend to criminal proceeds that have derived from another member state or a third country. Whereas the conduct of the individual or legal entity would be considered criminal activity.

These changes directly affect all obliged entities as we can observe increased corporate accountability with the shifting of responsibility to senior management and to the personnel of a corporation. Moreover, AMLA will directly supervise a limited number of selected obliged entities in the financial sector, from 2025 onward.

Companies operating in a transnational environment will need to take into consideration these changes and pay close attention to the determination of the source of funds of their clients, as well as the dual criminality factor. →

Most companies operating in the crypto sector have transnational activities. These activities will now need to be in line with FATF's Recommendations and Guidance, especially with Recommendation 15 (New Technologies), Recommendation 16 (Wire Transfers, also known as the 'Travel Rule'), and Interpretive Notes to them. Companies operating in the crypto sector will now need to have a proper licence (not just a registration for AML purposes) and collect originator and beneficiary information for all their digital assets – meaning they must know exactly where their assets are coming from and being sent to.

The use of Anonymity Enhanced Cryptocurrencies (AECs) or Privacy Coins should be avoided, and full tracing ability must be observed across the entire digital asset journey. The breaking of the tracing chain in the exchange (crypto to crypto exchanges) should also be avoided. Lifting the pseudonymity element and ensuring accurate identification of both originator and beneficiary of the assets can be challenging – especially for exchanges cooperating with un-hosted wallets. But there are solutions already available that can assist with tackling this issue.

### How is the EU addressing the challenges of regulating digital currencies and other emerging payment technologies in the context of AMLD6?

The AMLD6 is the EU Commission's modern, collaborative approach to fighting Money Laundering.

Despite there only being one direct mention of the term 'virtual currencies' in AMLD6, the fact that FATF's Recommendations are being taken into a particular account, practically means that the EU is in line with FATF Recommendations.

By aligning with Recommendation 15 (New Technologies), Recommendation 16 (Wire Transfers, also known as the 'Travel Rule'), and Interpretive Notes to them, the proper guidelines are being set for a more consistent and homogeneous approach. One can highlight the demand for Virtual Asset Service Providers (VASPs) or Crypto Asset Service Providers (CASPs) to apply customer due diligence measures when carrying out transactions amounting to EUR 1,000 or more and the added measures, as described in the previous question, to mitigate risks in relation to transactions with self-hosted wallets.

Moreover, the increased sanctions for non-compliance and the inclusion of legal entities in the liability spectrum is also a factor that could be potentially preventive for potential wrongdoing.

### What is the timeline for implementation of AMLD6, and what are the key milestones and deadlines that affected entities should be aware of?

3rd December 2020 was the date that Member States had to transpose the AMLD6 into their national laws, whilst businesses had a grace period that lasted until 3rd June 2021. Many countries have missed this deadline. On 7th December 2022, the Council agreed on a new position for closing possible loopholes in the existing regulatory framework. So, monitoring the website of the relevant regulator per jurisdiction is the appropriate path for this.

### How will AMLD6 be enforced, and what penalties or sanctions can be imposed for non-compliance?

AMLD6 will be enforced via the transposition of its provisions in the domestic legislation of each Member State, with the option for Member states to apply stricter rules. AMLD6 will also be part of the new EU AML Rulebook.

The sanctions that can be applied vary. In cases where the damage from the breach can be determined, the fine is at least twice the amount derived from the breach or a minimum of EUR 1 000 000.

In cases where the obliged entity implicated is a credit or financial institution, the fines for a legal person can mount up to at least EUR 10 000 000 or 10 % of the company's total annual turnover – as reported in the latest available accounts approved by the management body. If it's a parent or subsidiary, then the equivalent from the latest consolidated accounts is approved by the management body of the ultimate parent undertaking. In the case of a natural person, the fine is at least EUR 5 000 000.

Sanctions for companies that committed or attempted to commit money laundering, could include exclusion from access to public funding, confiscation of business assets, placement under judicial supervision, or even closure of business.

It is also implied that senior management may be held accountable for any subsequent money laundering if a company fails to implement AML/CFT measures effectively.

AMLD6 also amends the minimum imprisonment for money laundering offences from one year to four years. →

This is a very good indicator of the EU's efforts to tackle money laundering via harmonisation of the repercussions throughout the Member States and its commitment towards more sustainable economic growth for the Union.

### What steps can financial institutions and other affected entities take to ensure they are compliant with AMLD6, and what resources are available to support them in this process?

Firstly, compliance culture is the most important part. Compliance tone should always be given from the top, and this is the spirit of the AMLD6.

Secondly, financial institutions and other affected entities should ensure appropriate training is provided to their employees. Training helps with ensuring everyone across the organisation understands what AML/CFT is, how suspicious transactions or behaviour can be recognised, what is each employee's liability and what is at stake in case of non-compliance since it's a collective obligation.

Thirdly, via the update of their policies with the updated definitions, obliged entities are called to measure their exposure and risk, at both national and transnational levels, and ensure that enhanced transaction monitoring procedures and appropriate Customer Due Diligence and adverse media screening are in place.

Local nuances in the transposition should always be expected. Should an entity operate on a transnational basis, it should always consider the maximum jurisdictional approach.

Lastly, for best compliance practices, one should always consult the FATF Recommendations, as well as instruments of other international organisations and bodies active in the fight against money laundering and terrorist financing, in addition to AMLD6.



[nuvei.com](https://nuvei.com)

**Nuvei** is designed to accelerate your business. Our future-proof technology allows companies to accept cutting-edge payment options, optimise new revenue streams, and get the most out of their stack — all on one platform.

# Join the Fight Against Illicit Financial Flows: Building Peaceful and Ethical Societies Worldwide



*It is vitally important we do not get complacent or discouraged. If we lose sight of the victims, which is all of us, we may cease to be creative and passionate in identifying new approaches to detection.*

**Meagan Birch, MLRO & Head of Compliance**

# Fincrime Legends

Courage, Cake, and a Half-Eaten Hashbrown: What Does This Have to Do with Turtles?



**Meg** is an enthusiastic MLRO & Head of Compliance who wants to encourage the industry to challenge what we accept as effective now and always keep the victims (which is all of us) at the heart of our programmes.

**Meagan Birch** ■ *MLRO & Head of Compliance*



**Ray Blake** of the Dark Money Files is a former MLRO, now a speaker, writer, trainer, and podcaster on anti-financial crime matters.

**Ray Blake** ■ *Director of Dark Money Files*



**Ruth** operates at the nexus of finance, technology, and regulation and is passionate about creating the digital financial ecosystem of the future.

**Dr. Ruth Wandhöfer** ■ *Author, Speaker, Adviser & Coach*



**Dr. Mario Menz** is a social scientist, MLRO, and Head of Compliance. He specialises in behavioural change and organisational transformation.

**Dr. Mario Menz** ■ *Social Scientist, MLRO, and Head of Compliance*



**Dawn Fisher** is a current industry practitioner, an esteemed AML trainer, and a speaker/content contributor on AML and related topics.

**Dawn Fisher** ■ *Industry Practitioner, AML Trainer*



Given that we recently had Earth Month, can we talk about our impact on the environment? Do you remember the **video of the turtle** with a straw stuck in its nose? It galvanised the compassion of millions of people worldwide, and before we knew it, plastic straws became so unacceptable that we now have several alternatives which won't hurt turtles anymore.

***'It had a very emotional effect on people and it definitely fueled the movement that already existed.'***

In the turtle example, people – just like you and I, got active in creating new solutions. We harnessed a collective will and challenged big corporations to see the unintended yet harmful impact of their products and take our demand for change seriously. We would all benefit if we led a similar charge across Financial Crime Compliance (FCC).

Many people who work in Financial Crime Prevention began their careers with an ambition to 'do good'. Heck, when we were kids who didn't enjoy playing cops and robbers...and for some of us it even became a career. But somewhere along the way, the vast majority of us lost that sense of adventure and achievement that comes from catching the 'baddies'. The job might have even become hard work and a thankless task. That's no fun, right? And could we go as far as saying that because the current approach is so common, some of us might have given up trying to remedy the ineffectiveness?

About ten years ago, companies, regulators, and policymakers began using a new term: Financial Crime Compliance. Maybe we didn't notice the shift from Financial Crime Prevention? But herein lies a truth that many of my peers discuss openly. When did our collective ambition shift from Prevention to Compliance?

**Dawn Fisher** wrote to me: *'I don't know if it is truly appreciated that the shift from FCP to FCC is a paradigm shift from what should be our intended outcome to prevent financial crime (or the furtherance of financial crime via detection) to complying with our regulatory obligations to have in place a governance framework which is not proven to prevent financial crime but does tick boxes for compliance'*.

It is vitally important that we ask ourselves what our approach is to change and social activism. Many professionals in FCC strive to make a positive contribution to the fight against financial criminals. However, why have we accepted that all our current collective efforts to stop illicit financial flows are shockingly poor? The United Nations

Office on Drugs and Crime (UNODC) report is widely quoted: **less than 1% of global illicit financial flows are currently seized and frozen**. If we applied for a job and told the prospective employer, by the way, we're going to be hideously expensive, very noisy, and make the right decisions one-to-two percent of the time... do you think any of us would get hired? How depressing that is our current industry benchmark. It is therefore understandable that some could question the value of our current efforts. We might as well just join the swaths of companies producing hazard-light approaches to financial crime compliance and admit defeat.

**Ray Blake**, the director of **Dark Money Files** added that company executives make multiple choices that directly impact effectiveness. *'Faced with what they perceive as the high cost of either hiring capable people or training people to become capable, most firms choose instead to hire inexperienced, less capable people, and keep them in that state. It's about seeing KYC and the other routine compliance obligations as low value and a drain on costs. So, it's afforded minimal development'*.

First, we have to admit there is far more we can do and that it's time to have an introspective look at things we may be doing that contribute to low effectiveness. I'd like to assert that we may have an attitude problem. Countless boardrooms discuss the high costs of AML and Compliance. That is a concern a business needs to evaluate critically. However, all AML & Compliance professionals must prove their worth not just through legal necessity to comply but also in terms of how we can improve sustainable development for the companies we work for. Perhaps now is the time to investigate our motives and what we are each doing to PREVENT & DETECT financial crimes. Is this all we can do?

However, it is vitally important we do not get complacent or discouraged. If we lose sight of the victims, which is all of us, we may cease to be creative and passionate in identifying new approaches to detection. In 2022, the UN confirmed the importance of the reduction of illicit financial flows (IFFs) as a priority area to build peaceful societies around the world, as has been recognised in the **2030 Agenda for Sustainable Development**. Perhaps, if we have an agreed way to meaningfully identify, measure, and track our collective effectiveness we will ignite global willingness to combat it at the root. →

Fincrim professionals openly share mutual frustrations. Some think the industry is doing the best it can whilst others want to radically change our approach but get overwhelmed with the sheer size of the task if we really want to be effective. *'At the same time, the effective and efficient use of technology has been a challenge, as not many solutions truly address the needs of the FCC community in the right way'*, says **Dr. Ruth Wandhöfer**.

We were joking about cake and half-eaten hash browns as an illustration of our Financial Crime Compliance programmes and controls. We joked that our Transaction Monitoring systems were like half-eaten hash-browns and not very nourishing, that our compliance programmes were rarely as welcome as cake when shared in the office and that the office caterers (MLRO) had just resigned because anything they served was never good enough. We laughed but it got us thinking, critically, about how we have ended up in such a mess in FCC.

There are countless articles, lectures, and webinars talking about the burdens faced by those working across regulatory compliance. The burden of keeping abreast with current regulatory change and corporate frustration. The burden of filing suspicious activity reports, the burden of understanding the technological advancements that are being used in many technical solutions, and the sheer burden of the volume of work to do. We rarely hear the word compliance in ML in the same sentence as fun. And maybe that's part of what's missing. As kids, most of us enjoyed playing good guys versus bad guys, but do we still bring that useful exuberance to our jobs as MLROs? Can we truly say we wake up eager to catch the bad guys? Or do we envision our day as a series of meetings, political arguments, and requests for help that may go unresolved? Are we completely resigned before we even begin? Are we too afraid to challenge ourselves because we risk failing or losing our professional reputation in the process? Are we too afraid to admit our fears and flaws so we just keep doing what everyone else does but sacrifice making a real difference to effectiveness? When did we stop being courageous in our endeavours in favour of being comfortable?

I like fables – they ignite the imagination, and each reader can apply the lesson differently. When working with people in FCC I always suggest an important book to read called **'Who moved my cheese?'** I'm sure you've heard of this popular book by now – if not, read it. The TL: DR is that change happens, prepare for it, and embrace it. What if we brought this simple idea to bear in financial crime compliance?

**Dr. Mario Menz** suggested two questions. *'First, what's the goal of FCC? There are at least two and sometimes we focus on one more than on the other. The second question is what motivates people to do a good job as an FCC professional? Or in other words, where do they get job satisfaction from? Some people may not know they are complicit because of their goals'*.

*'There is a much higher tolerance to white-collar crime than to street crime. Why? Because we are all able to identify with the stabbing or mugging victim. We have an emotional response because that victim has a face, and it could have been us. But when it comes to white collar crime (like money laundering) we find it much more difficult to empathise with because we can't see the victim. There is no immediate emotional response because we can't see ourselves as the victim'*.

If you follow this train of thought, you could argue that FCC competencies and commitments will change if we put the victims of fincrime at the heart of what we do by helping people understand that it could have been them and how IFFs affect us all.

Perspective is decisive – so, if you think you can or think you can't, you'll prove yourself right. Your perspective can also be a source of your power or your prison. It's time for our industry to choose: do we just keep following a vision that does not resonate with our goals or can we focus on what inspired our career choice and collectively identify and try new approaches to make a difference? Let's find the straws in our Financial Crime PREVENTION approaches and create new ways to be effective against the 'baddies' who rob us all of peaceful communities. Let's turn the tide against complacency and illicit financial flows. But please, don't lose your inspiration to keep trying, every day. We won't get to 100% effectiveness overnight, but each incremental improvement changes the lives of countless victims worldwide and is worth striving towards! Be passionate, be bold, and be courageous in the ways you detect and prevent financial crime – it's what is missing and will make a real difference!

# Banking Circle

## Compliance to the Rescue



**Mitch Trehan** is the UK Head of Compliance and MLRO at Banking Circle and a regular public speaker. Co-chair of the 'Interbank Payment Policy Committee' for UK Finance and on the Payments Association Advisory Board. Named 'One to Watch' by Money 20/20.

Mitch Trehan ■ UK Head of Compliance and MLRO ■ Banking Circle

*Often seen as an inconvenience, a burden, or a blocker programmed to say 'no' to every new idea, regulatory compliance has been given a bad name. Here, Mitch Trehan, UK Head of Compliance and MLRO at Banking Circle reminds businesses that compliance exists to save lives and livelihoods, not to put a stop to innovation.*

Compliance. The final tick box before a new product, service, or announcement goes live. Right? For a long time, this has been the case, but this approach of bringing compliance on board at the end of the process has stunted innovation and, in my view, has unfairly earned those with compliance in their job title a bad reputation for saying 'no' to exciting new projects. As a result, many firms see compliance as a blocker rather than an integral part of the business strategy.

This attitude is one of the most significant compliance challenges today. Presented with a fully developed solution, the team tasked with protecting the business, its clients, and its customers may discover non-compliant elements that must be resolved before the project can launch. Product development must then be put into reverse to fix the issues.

An inexperienced baker would be foolish to glance briefly at a list of ingredients and attempt to bake a cake without following a recipe step-by-step. In the same way, those who are not experts in compliance should rely on the experienced compliance officer during product development to ensure the end product is compliant and ready for launch – like the best Mary Berry Victoria sponge.

### Resetting reputations

The forgotten truth is that a compliance officer's job is not to say 'no' – unless the request is illegal, of course. Their job is to advise on the policy and stance of a business and to explain the risks and the options. If the business wants to do something new, a compliance officer should not stand in the way without just cause.

However, compliance needs a seat at the table from the outset. Then it will be positioned to support product development and ensure solutions and positioning are correct and compliant from the start, avoiding wasting time and resources redesigning 'finished' solutions. Bringing in compliance at the end, as a box-ticking exercise, is a strategy known to fail. As such, organisations need to reframe how all employees see compliance, and how it fits into the business, from the top down.

### External challenges

Ongoing regulatory changes bring significant costs and burdens to any business. Each change requires additional training and checks on current products, services, and processes. Updates and tweaks may be required, costing more time and money, and potentially incurring downtime while changes are implemented.

A 2023 report from LexisNexis Risk Solutions entitled '**True Cost of Compliance**' recently revealed the staggering cost of financial crime compliance for UK financial services – approximately GBP 34.2 billion in 2022, or an average of GBP 194.6 million per business per year. Survey respondents cited increasing regulation and regulatory expectations as the greatest external drivers of cost. →

The speed of regulatory evolution is not only financially costly, but it also creates a skills challenge. As requirements shift, there are fewer and fewer individuals who can be called upon as experts in the field, to advise and support in addressing the changes.

### The compliance big picture

It is often forgotten that financial regulation is in place to protect consumers and businesses and to help stop terrorism. It is not there to be an inconvenience; it is there for the greater good. Therefore, businesses employing robust compliance measures and processes are doing the right thing for society at large – compliance is a moral and sociological obligation.

It is also fundamental to a business' reputation. Who can forget the enormous fine paid by HSBC back in 2012 when the bank's inadequate compliance and Anti-Money Laundering processes failed to stop criminals and terrorists from laundering money through it?

Not only is reputation vital for customer confidence, but it also helps attract and retain the best workforce. Younger generations joining the industry are more focused on doing the right thing, so a business committed to robust compliance will fit well with its values and will be an attractive potential employer. Customers too want to work with a business they know is doing the right thing.

I believe that as soon as a business truly makes compliance integral to operations, more of the workforce wants to be involved. The business then quickly gains economies of scale, where its people have the right culture and conduct. With a shared focus on compliance across all aspects of the business, expertise is shared, people learn more quickly and become more efficient, and compliance naturally becomes less of a burden.

### Looking ahead

The encouraging news is that businesses do seem to be changing their ways and learning from their mistakes. The LexisNexis Risk Solutions report states that businesses are investing in making improvements to their compliance processes and anticipate seeing tangible business benefits by 2025, including higher customer acquisition rates and better financial crime detection rates.

Many businesses are also putting compliance officers on the management team. The fact is, in the UK the minimum number of people within a business who must always be authorised by the regulator are the head of the business or branch manager and the Money Laundering Reporting Officer. That short list clearly demonstrates the importance of the role.

No business wants to be caught out and fined by the regulator, so they must remember that while they have historically seen compliance as a box-ticking exercise at the end of product development, that is certainly not how the regulator sees it. Compliance is a vital and valuable requirement and must be handled as such.

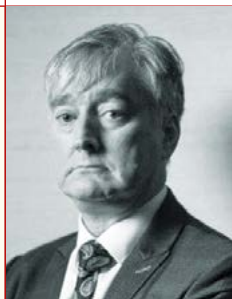


[bankingcircle.com](https://bankingcircle.com)

**Banking Circle** is a fully licenced next-generation Payments Bank, designed to meet the global banking and payments needs of payments businesses, banks, and online marketplaces. Banking Circle solutions power the payments propositions of 300 financial institutions across the globe, including 16 banks.

# Global Compliance Institute

**Martin Woods, Cashplus and Global Compliance Institute (GCI) Chair, stresses the importance of working with trained/skilled people in the fight against fincrime.**



**Martin Woods**, former financial crimes detective, is the chair of the Global Compliance Institute advisory panel. He's a Senior Compliance Officer with experience all over the world, providing training to regulators and firms. He advocates we are all here to Make A Difference and he is always on the lookout for those who may want to join his MAD – Make A Difference revolution.

Martin Woods ▪ Chair ▪ Global Compliance Institute

Many times, at fincrime conferences, people complain of the lack of a trained staff or unskilled workforce working in the field of compliance. What has been your experience so far related to this topic?

**Putting the wheels on the AML suitcase** – there are lots of wonderful, smart, enthusiastic, and talented young people in this industry. They have a very important role to play in the development of AML. Here's the context: many years ago, when I was but a small boy, my dad would often carry two big suitcases when we went on holiday. Upon arriving at our final destination, dad would be a little fatigued, sometimes irritable and commonly sweaty.

Why so? You ask. Well, it was because he carried the suitcases, as back then suitcases had no wheels. Imagine, if you will, the lunacy of suitcases without wheels. It references the simplicity of some wonderful solutions and innovations. Back to 2023 and the modern-day world of AML, it's not working, it is all too often, ineffective, and inefficient. Thus, it is the role of these smart young people to put the wheels on the AML suitcase and I am looking forward to seeing it in action, one day.

*“ There are lots of wonderful, smart, enthusiastic, and talented young people in this industry. They have a very important role to play in the development of AML.*

What are the causes of this lack of skilled/trained people?

Notwithstanding the above, there are not enough trained AML professionals, moreover, some have not been trained properly and worse still, some think they do not need training. I am older and may not be wiser, but I know I can learn more and I want to learn more. Only the fool thinks he knows everything. Smart and talented AML professionals are much sort after and consequently, they are expensive. Historically there has been a threat of prison for managers, executives, and even AML professionals themselves if they fail to implement an appropriate AML programme, but no one goes to prison. This has influenced decision-making, resource allocation and expenditure.

The fact is AML is not such a high risk for individuals and therefore it is not a priority. But change is on the horizon, new laws in the UK will commercially punish banks/firms who fail to stop money laundering. They will be presented with a 50% liability of fraud losses incurred by victims who have funds stolen from other banks/firms and subsequently laundered through the penalised bank. Now we are talking, we are talking loud and clear, money laundering is a very high commercial risk and must be stopped. This will improve training, otherwise, money laundering will continue and losses will increase. →

## How can experts build the practical skills they need to keep up with all the latest industry and technological developments in the ever-evolving compliance arena?

Don't get ahead of yourself, start with the basics and build. The foundation of AML is KYC, so who is a bank's/firm's customer? Take a look in the mirror – there you go, you are a customer. What do we know, you know about you? What is hidden? You and your accounts are the benchmarks, you are not money launderers, and you now know what a money laundering account does not look like. You are not alone; most people are like you. As to others, the basics are, can you, can they prove who they are? Can they prove where they state they reside and for companies, can they prove they do what they purport to do? Now, how difficult is that? If your customer is a British Virgin Islands (BVI (Beneficiaries Virtually Invisible)) company, you and your firm are not compelled to do business with them.

Accounts – use yours as a benchmark, be prepared to challenge, but recognise what you are seeing when looking for suspicious transactions. What if no money laundering is taking place in most instances? Focus and be prepared to miss some money launderers, this is what risk-based means.

## What can be challenging in achieving this?

Stubborn people who think they know better and others who assert the status quo works, because they have always done it that way. Even though they have done it badly.

## Once this holy grail is achieved, what are the other beneficiaries, besides the direct ones, the people trained?

There is no holy grail, money laundering is an incurable virus which mutates. We will be fighting the launderers forever.

## To sum up, what advice would you give regulated entities to build successful compliance programs in general?

Step back, find time to get away from putting out the fires and design better controls, a new fire engine, fire breaks, etc. Look at your programme, if there are no wheels it is ineffective and inefficient.



[gci-ccm.org](http://gci-ccm.org)

**Global Compliance Institute (GCI)** is an International Financial Crime Prevention and Compliance Training Institute based in Australia but operating globally. We specialise in Compliance and combatting Financial Crime, including Anti-Money Laundering and Counter-Terrorism Financing, in addition to KYC, Sanctions and Embargoes, Regulatory Compliance Management, FATCA, and CRS.



# Spotlight on Financial Crime and Fraud Fighters: the Leading Experts and Innovators in the Industry



*Regtech's place and worth will only increase as more businesses turn to regtech solutions and digital transformation initiatives to change the way financial services organisations operate at scale.*

**Alex Ford, Director, The RegTech Association**

# Mirela Ciobanu

Exploring Regtech, IDV Fundings & Mergers – Insights into Current Trends and Future Projections



**Mirela Ciobanu** is Lead Editor at **The Paypers**, specialising in the Banking and Fintech domain. With a keen eye for industry trends, she is constantly on the lookout for the latest developments in digital assets, regtech, payment innovation, and fraud prevention. Mirela is particularly passionate about crypto, blockchain, DeFi, and fincrime investigations, and is a strong advocate for online data privacy and protection. As a skilled writer, Mirela strives to deliver accurate and informative insights to her readers, always in pursuit of the most compelling version of the truth. Connect with Mirela on **LinkedIn** or reach out via email at **[mirelac@thepayers.com](mailto:mirelac@thepayers.com)**.

Mirela Ciobanu ▪ Lead Editor ▪ The Paypers

*'All catastrophes have the same effect: they sharpen our understanding of our interconnectedness and mutual dependency, they clarify our values, they encourage us to rethink our priorities, they expose our prejudices, and they build our resilience.'* — Hugh Mackay, Australian psychologist, social researcher

Until some time ago, most funding and M&A articles started with encouraging market statistics, stressing the market's potential for growth. However, for the last several months, a series of severe and mutually reinforcing shocks — the COVID-19 pandemic, the war in Ukraine and resulting food and energy crises, surging inflation, debt tightening, as well as the climate emergency — have battered the world economy, making it harder to anticipate what will happen next.

The funding and M&As market in 2022 and Q1 2023 has been dominated by a few key ideas. Firstly, **daily headlines about layoffs have become increasingly common**, with **more than 94,000 workers in US-based tech companies** (or tech companies with a large US workforce) being laid off in mass job cuts so far.

Secondly, **some companies that became unicorns in the past were found to have no substance** (FTX), leading to a reckoning in the market. **According to CB Insights**, global funding in Q3 2023 amounted to USD 74.5 billion, which is less than half the total funding received in 2021. The report highlights a 34% quarter-over-quarter decrease in funding. **In Silicon Valley, funding hit its lowest level since Q4 2019**. Despite some startups managing

to weather the economic downturn, several were acquired, and a few collapsed in 2022 (Manchester-headquartered neobank Bank North, Israeli AI startup BeyondMinds, Berlin-based security token startup Neufund, etc.). The outlook for 2023 appears as bleak as Railsbank, a former star of the UK payments industry that reportedly raised over USD 100 million from investors, **has been purchased and re-capitalised by a consortium**, due to mounting financial and regulatory challenges, **according to Bloomberg**.

Thirdly, over the past 14 months, the **average funding deal has decreased**. Looking back at **past funding and M&A activity in the regtech and IDV sector**, several startups received over USD 200 million in 2021, such as Socure, Feedzai, Incode, and others. However, in 2022 and 2023, we have seen a decline in funding amounts, with the largest IDV funding reported by The Paypers being Veriff's USD 100 million.

Despite the turmoil of the past year, **there is still growth potential in the regtech sector**. In 2022, the regtech sector, globally, saw an increase in venture capital, private equity, and M&A investments, reaching a total value of USD 18.6 billion. This represents a notable increase compared to the previous year's total of USD 11.8 billion, despite a slight decrease in the number of deals from 380 to 315, **according to Statista**. *It is worth noting that the value of investments in the fintech sector decreased significantly in 2022, making the increase in regtech investments even more surprising.* →

Nevertheless, we inhabit an interconnected world where various components have a significant impact on one another. Even if some sectors or regions are performing well, negative developments in other areas could potentially impact the entire system.

## Digital identity and identity verification trends that are influencing Identity Verification (IDV) fundings & mergers

Digital identity and identity verification are crucial aspects to consider when discussing digital transformation, payment innovations, and transitioning to web3. Considering people are connected via multiple devices and platforms, verifying the identity of the other party has become increasingly important. As a result, several developments are happening in this space that warrants attention.

- *Digital transformation in many sectors is accelerating, driving technology adoption;*
- *Young digital identity startups are leaving the market and are being acquired by established, larger competitors;*
- *The current competition among banks and bigtechs over digital wallets is stressing the importance of digital identity;*
- *Many businesses are adding behavioural analytics and biometrics to product development to boost UX, while securing transactions;*
- *Businesses are increasingly adopting generative AI solutions;*
- *The evolution of the reusable identity market is seen as an important layer to building web3;*
- *Privacy and data protection laws are becoming more stringent worldwide;*
- *Regulatory updates around digital identity and customer data across the globe (eIDAS 2.0 in the EU, the Revised Digital Identity Guidelines from NIST in the US, Chinese Banking and Insurance Regulatory Commission's (CBIRC) new rules on consumers' rights and interests, etc.);*
- *The rise of decentralisation in finance, communication, entertainment, and other industries is driving the demand for user control over personal data. This has resulted in the widespread adoption of Self-Sovereign Identity (SSI) solutions.*
- *There is a noticeable interest in the crypto industry;*
- *Shifting to greener energy, quantum computing breakthroughs might influence the development of digital identity solutions.*

Having reviewed some of the factors shaping the digital identification market, let's explore some of the major trends currently dominating the regtech industry.

## Regtech and transaction monitoring trends

- *Financial institutions are searching for solutions to navigate the economic impact of the ongoing war in Ukraine, which includes sanctions and disrupted supply chains, as well as compliance risks and potential threats to all industries.*
- *The high inflation and the rising cost of living are leading individuals to fall prey to scams and even turn to criminal activities such as money laundering or committing fraud to make ends meet.*
- *The increase in digital onboarding in the financial sector provides a more efficient and cost-effective onboarding experience for customers and financial institutions while also reducing the risk of fraud.*
- *The impact of the use of cryptocurrency on AML programs*
- *The latest regulatory updates around crypto (MiCA), APP fraud, Ultimate Beneficiary Ownership (UBO), sanctions screening, and AMLD6*
- *The rise of global sanctions.*

These turbulent factors are driving significant changes in the funding and M&A landscape; but to be able to anticipate what will happen next and make the right investment or partner with the most suitable technology provider, it is also worth paying attention to some trends that will shape up the regtech and IDV industry.

## 2023 Regtech & IDV predictions

### The rise of new integrated identity platforms

To accelerate their growth in a challenging economic environment, many early-stage young digital identity companies with a few million dollars in annual revenue will likely be acquired by larger platforms in 2023. This will result in the emergence of a new class of integrated identity platforms that provide end-to-end solutions for the entire customer lifecycle.

### Increased adoption of biometrics in financial services

Product managers face the challenge of balancing user experience and security as consumers increasingly use physical biometrics, such as fingerprint scanning, for unlocking devices, verifying payments, and other purposes. This trend is particularly strong among younger consumers who demand instant access to information and services on their devices. →

As a result, businesses are increasingly incorporating behavioural analytics and biometrics into their product development to improve the user experience and enhance transaction security. This trend is expected to continue and become even more crucial by 2030.

*The rapid adoption of generative AI solutions has led regulators worldwide to concentrate on regulating AI, starting with AI accountability, AI explainability, and its impact on consumers and businesses.*

The rise of AI and machine learning is transforming the way businesses operate, and regulators are beginning to take notice. While the US lacks comprehensive federal AI legislation, there are various frameworks and proposed regulations in place that organisations must comply with. Meanwhile, the **European Commission's proposed AI Act** assigns AI applications to three risk categories and has the potential to become a global standard like the GDPR. However, the law has some limitations, such as loopholes and a lack of flexibility. As AI continues to play an increasingly significant role in society, businesses must stay informed and compliant with regulations.

*The existence of data protection and user protection laws, especially those that promote a safe online environment for children, is expected to drive the creation of data privacy/protection startups.*

### **Wider adoption of SSI solutions**

By using SSIs in finance, users can maintain their privacy and control over their data while also securely participating in financial activities. Additionally, SSIs can help prevent fraud and other malicious activities by allowing users to prove their identity without revealing any unnecessary personal information. SSI solutions perfectly match GDPR-like regulations and users' demand for privacy, and such, we anticipate this sector to grow more.

### **Digital identity will emerge as a critical element in digital wallets, crypto, and Web3**

*Banks should not compete with bigtech on payments but focus on identity to expand their wallet's ecosystem and make it an essential offering.* **A report by the Mobey Forum** highlights that digital identity is a critical factor in the emerging digital economy, and recommends banks become trusted intermediaries in the digital identity ecosystem. To do this, banks should leverage their role as custodians of personal data to provide additional value through digital identity services.

Cryptocurrencies are built on blockchain technology, which offers a decentralised and tamper-proof way of recording transactions. This technology can also be applied to digital identity verification, allowing for a more secure and private way of verifying identities. One example of this is the concept of self-sovereign identity (SSI).

Crypto's influence on digital identity lies primarily in its potential to provide secure and decentralised identity verification systems. Digital identities that are built on decentralised identity (DID) systems, enable users to create, manage and authenticate their identities across multiple Web3 applications and services without relying on a central authority.

*The surge of activity and announcements in the realm of crypto adoption and regulations (MiCA), APP fraud, Ultimate Beneficiary Ownership (UBO), sanctions screening, and AML.*

*The rise of global sanctions is another trend that organisations must be aware of and prepared to comply with. Financial institutions must ensure they have the necessary systems and processes in place to comply with current sanctions and be able to quickly adapt to any changes in the future.*

### **Shifting to greener energy might influence the development of digital identity solutions (transition to the cloud, as an energy-saving option)**

As more and more data are collected and processed in digital identity systems, the energy consumption required to secure and maintain these systems can also increase. This may lead to a greater emphasis on energy-efficient and secure data storage solutions, such as cloud computing, which can reduce energy consumption and improve data security. However, *the demand for energy-intensive technologies like blockchain and cryptocurrency mining may shift to renewable sources of energy.*

### **Quantum computing to influence the development of digital identities**

The development of quantum computing could have both positive and negative effects on digital identity. On one hand, quantum computing could potentially lead to stronger encryption methods that could make digital identities more secure. However, on the other hand, quantum computing could also potentially break current encryption methods, allowing hackers to gain access to sensitive information, such as digital identities. →

This means that digital identity systems must be updated and strengthened to resist quantum-based attacks and there is a need for further research and development to ensure that digital identities remain secure in the face of the emerging quantum computing technology.

## The Financial Crime and Fraud Report 2023 Industry Mapping

All in all, with the emergence of more regulations surrounding data protection, the use of advanced technologies such as biometrics, AI, and blockchain to enhance user experience and identity security will become increasingly common. Furthermore, hot debates around crypto, APP fraud, sanctions screening, and AI accountability are likely to result in an increasing regulatory landscape complexity, while the recession in some parts of the world is expected to lead to a surge in fraud.

As such, the Financial Services sector has identified areas where they want to see improvements delivered in the future, including increased efficiency and speed, cost savings, and accurate data analysis for decision-making. *Technologies such as AI, ML, and data analysis, as well as solutions providers such as regtechs and fintechs, are being used to meet these needs.*

To help you find the right partner, The Paypers has created an **Industry Mapping** that highlights the most relevant companies and their capabilities in areas such as fraud and risk management, identity verification, and digital onboarding. **The Financial Crime and Fraud Report 2023 Industry Mapping** focuses on solution providers that are part of the digital onboarding and financial crime ecosystems. The mapping includes sections on fraud and financial crime hubs, transaction fraud, account fraud, ATM fraud, AML transaction monitoring, KYC/CDD, KYC remediation, digital identity service providers, identity verification, and authentication.

Don't miss our company profile section, which provides details about offerings, business partners, referrals, awards, and more offered by our collaborators to regulated entities such as banks, fintechs, brokers, crypto exchanges, blockchain and crypto companies, merchants, and marketplaces, PSP, acquirers, and telecoms.

*Also, if you're interested in learning more about the most significant investments and partnerships that have made headlines in The Paypers during 2022 and Q1 of 2023, we encourage you to read our articles covering **Regtech & Identity Verification Buys & Funding Analysis in Europe, Regtech and IDV M&A and investments in the US and Canada**, and **2022/2023 Regtech and IDV Buys & Investments Analysis in Asia, LATAM, and Africa**. These articles offer detailed analyses of the investments and partnerships that have shaped these industries and provide a glimpse into the trends that are likely to dominate the market in the coming years.*



# The Key Players in the Battle Against Financial Crime and Fraud

Fraud and financial crime hub – decisioning platform



Transaction fraud



Account fraud



Financial crime data provider and intelligence



AML transaction monitoring



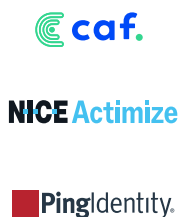
KYC / CDD



KYC remediation



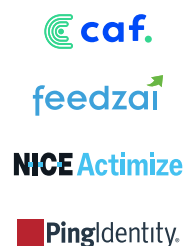
Digital identity service provider



Identity verification



Authentication



Researched by © The Payers, 2023








# Company Profiles



Company		Caf		
		Caf offers identity verification, onboarding, and authentication solutions to digital businesses to help secure their customers' journey. Our comprehensive suite of identity solutions enables the verification of individuals and businesses and is designed to accommodate the unique requirements of both regulated and non-regulated businesses.		
<b>Background information</b>				
Year founded	2019			
Website	<a href="https://www.caf.io/">https://www.caf.io/</a>			
Target group	<ul style="list-style-type: none"> <li>• Banks/FS/Brokers</li> <li>• Fintech</li> <li>• Crypto exchange/Blockchain and crypto companies</li> <li>• Merchants/Marketplaces (regulated entities)</li> <li>• PSP/acquirers</li> <li>• Telecom</li> <li>• Streaming platforms/Social Media Content Creators/ Gambling</li> </ul>			
Supported regions	Global			
Contact	Vanita Pandey			
Company's motto	Enabling business to know their everything			
Member of industry associations and/or initiatives	MRC, Liminal			
<b>Core solution</b>				
Core solution/problems the company solves	<ul style="list-style-type: none"> <li>• Fraud and financial crime hub - decisioning platform</li> <li>• Account fraud</li> <li>• Financial crime data provider and intelligence</li> <li>• AML transaction monitoring</li> <li>• KYC/CDD</li> <li>• KYC remediation</li> <li>• Digital identity service provider</li> <li>• Identity verification</li> <li>• Authentication</li> <li>• KYB - business verification</li> </ul> Solving customer onboarding, authentication, consumer/business verification, and fraud prevention use cases.			
<b>Technology</b>				
	Native cloud			
<b>Data input</b>				
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>	
Identity document scanning			x	
Personally Identifiable Information (PII) validation			x	
Email verification		x		
Phone verification		x		
Credit check		x		
Compliance check		x		
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>	
Physical biometrics			x	
Device fingerprinting	x			
Geo-location		x		
Remote access detection		x		

Mobile app push		x	
One-time passwords	x		
Knowledge-based authentication		x	
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Abuse list	x		
Financial crime data	x		
Sanctions data (sanctions, enforcements, PEP, and adverse media)	x		
Watchlist screening	x		
Address verification	x		
Credit bureau	x		
Information sharing	x		
<b>Methodology</b>			
Machine learning	Hybrid		
<b>Decisioning</b>			
	<ul style="list-style-type: none"> <li>• Manual review</li> <li>• Case management</li> <li>• Decision orchestration</li> </ul>		
<b>Business model</b>			
Pricing model	Pricing is per transaction and based on volume and complexity.		
Fraud prevention partners	Clearsale, Neoway, Incognia		
Investors	Multiple leading VCs and private investors		
Year-over-year growth rate	~100%		
Number of employees	330		
Future developments	Decentralised identity network, ongoing enhancements to the know your everything platform.		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		

# Know Everything About Every User, Wherever They Interact With You



**In today's digital world, businesses need to be vigilant in knowing everything about their users at all times.**



That's where Caf's Know Your Everything platform comes in. We deliver automated and highly accurate identity verification solutions, so you can serve your customers with a more personalized and deeper relationship across all touchpoints while eliminating fraud.



Talk to one of our experts today to learn more.





Company		Ekata, a Mastercard company	
		<p>Ekata, a Mastercard company, empowers businesses to enable frictionless experiences and combat fraud worldwide. Our identity verification solutions are powered by the Ekata Identity Engine, which combines sophisticated data science and machine learning to help businesses make quick and accurate risk decisions about their customers. Using Ekata's solutions, businesses can validate customers' identities and assess risk seamlessly and securely while preserving privacy. Our solutions empower more than 2,000 businesses and partners to combat cyber fraud and enable an inclusive, frictionless experience for customers in over 230 countries and territories.</p>	
<b>Background information</b>			
Year founded	2019		
Website	<a href="http://www.ekata.com">www.ekata.com</a>		
Target group	<ul style="list-style-type: none"> <li>• Banks/FS</li> <li>• Fintechs</li> </ul>		
Supported regions	Global		
Contact	Heather McKay		
Company's motto	Global identity data and insights to reduce friction, improve conversions, and combat fraud		
<b>Core solution</b>			
Core solution/problems the company solves	Identity Verification		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Small transaction verification	x		
Email verification	x		
Phone verification	x		
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Geo-location	x		
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Address verification	x		
<b>Methodology</b>			
Machine learning	<ul style="list-style-type: none"> <li>• Supervised ML</li> <li>• Unsupervised ML</li> <li>• Hybrid</li> </ul>		
<b>Decisioning</b>			
	Manual review		
<b>Business model</b>			
Pricing model	More information available upon request		
Year-over-year growth rate	More information available upon request		
Number of employees	More information available upon request		
Future developments	More information available upon request		
<b>Customers</b>			
Customers reference	More information available upon request		
		View company profile in online database* 	
		<p>*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a>.</p>	





*A challenger bank saw a **42% increase** in new accounts by improving its customer onboarding process with Ekata.*

*Ekata's award-winning Identity Engine<sup>®</sup> uses verified global identity data that helps you approve more good customers, optimize the customer experience, and increase revenue from customer loyalty.*

*Leverage the power of the Ekata Identity Engine to make faster risk decisions and accept more good leads today.*

[CONTACT US TO LEARN MORE](#) 

Company		Feedzai	
		<p>Feedzai is the world's first RiskOps platform, protecting people and payments with a comprehensive suite of AI-based solutions designed to stop fraud and financial crime.</p> <p>Feedzai enables leading financial organisations globally to safeguard trillions of dollars of transactions and manage risk while improving their customers' trust.</p>	
<b>Background information</b>			
Year founded	2011		
Website	<a href="https://feedzai.com">feedzai.com</a>		
Target group	<ul style="list-style-type: none"> <li>• Banks</li> <li>• Fintechs</li> <li>• PSP/Acquirers</li> </ul>		
Supported regions	US, Europe, Middle East, APAC, Africa, LATAM, India, Global		
Contact	Joanna Akers-Khan		
Company's motto	Keeping Payments Safe		
Member of industry associations and/or initiatives	UKF, GASA, ACFCs		
<b>Core solution</b>			
Core solution/problems the company solves	<ul style="list-style-type: none"> <li>• Transaction fraud</li> <li>• Account fraud</li> <li>• Behavioural biometrics and malware protection</li> <li>• AML transaction monitoring</li> <li>• KYC/CDD</li> <li>• Authentication</li> </ul> <p>Feedzai enables financial institutions keep payments safe by securing the end-to-end customer lifecycle by treating people as individuals and identifying bad actors and suspicious activity.</p>		
<b>Technology</b>			
	<ul style="list-style-type: none"> <li>• Cloud-enabled</li> <li>• Native cloud</li> <li>• On-premise</li> </ul>		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Behavioural biometrics	x		
Physical biometrics		x	
Device fingerprinting	x		
Geo-location	x		
Remote access detection	x		
Mobile app push	x		
3-D Secure 2.0		x	
Hardware token		x	
One-time passwords		x	
Knowledge-based authentication		x	
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Abuse list		x	
Financial crime data		x	
Sanctions data (sanctions, enforcements, PEP, and adverse media)		x	
Watchlist screening	x		

Address verification		x	
Credit bureau		x	
Information sharing		x	
<b>Methodology</b>			
Machine learning	<ul style="list-style-type: none"> <li>• Rule-based</li> <li>• Supervised ML</li> <li>• Unsupervised ML</li> </ul>		
<b>Decisioning</b>			
	<ul style="list-style-type: none"> <li>• Manual review</li> <li>• Case management</li> <li>• Decision orchestration</li> </ul>		
<b>Business model</b>			
Pricing model	Pricing is per transaction or account		
Fraud prevention partners	None		
Investors	Feedzai's main investors include KKR, Oak HC/ FT, Sapphire Ventures (SAP), and Capital One.		
Year-over-year growth rate	30%		
Number of employees	650		
Future developments	Identity Verification, multi-cloud		
<b>Customers</b>			
Customers reference	Capital One, Fiserv, ABN- AMRO, Pay-U, Citibank, Goldman Sachs, Mox		
	View company profile in online database* 		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		



# End-to-end protection from fraud and financial crime

- Account Opening
- Digital Trust
- Transaction Fraud
- Anti-money Laundering

**\$900M+**

**Consumers** protected worldwide

**\$500M+**

**Fraud** stopped yearly


**2T+**

**Events** processed yearly

**19B+**

**Transactions** monitored yearly

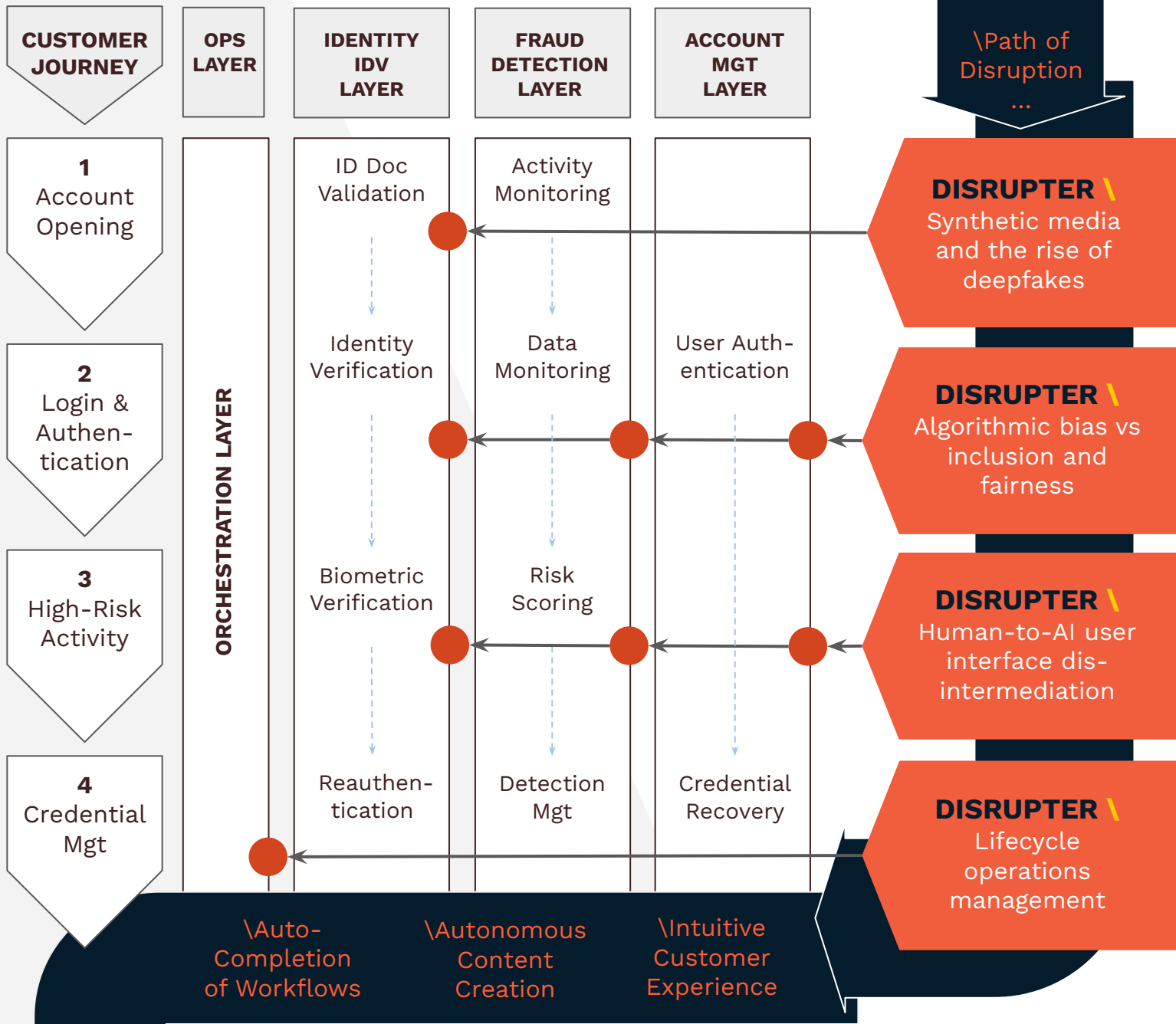


Company		IDVerse, an OCR Labs Company	
		IDVerse, an OCR Labs Company helps you quickly scale your business globally. Our fully-automated solution verifies new users in seconds with just their face and smartphone – in over 220 countries and territories with any ID document – without the burden of human intervention.	
<b>Background information</b>			
Year founded	2018		
Website	<a href="https://idverse.com/">https://idverse.com/</a>		
Target group	<ul style="list-style-type: none"> <li>• Banks/FS</li> <li>• Fintech</li> <li>• Brokers</li> <li>• Crypto exchange/Blockchain and crypto companies</li> <li>• Merchants/Marketplaces (regulated entities)</li> <li>• PSP/acquirers</li> <li>• Telecom</li> </ul>		
Supported regions	Global		
Contact	<a href="mailto:hello@idverse.com">hello@idverse.com</a>		
Company's motto	We empower true identity for people around the world.		
Member of industry associations and/or initiatives	More information available upon request		
<b>Core solution</b>			
Core solution/problems the company solves	Identity Verification Our fully-automated solution verifies new users in seconds with just their face and smartphone – in over 220 countries and territories with any ID document – without the burden of human intervention.		
<b>Technology</b>			
	Hybrid		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Identity document scanning	x		
Personally Identifiable Information (PII) validation	x		
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Physical biometrics	x		
Device fingerprinting	x		
Geo-location	x		
Remote access detection	x		
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Abuse list		x	
Financial crime data		x	
Sanctions data (sanctions, enforcements, PEP, and adverse media)		x	
Watchlist screening		x	
Address verification		x	
Credit bureau		x	




<b>Methodology</b>	
Machine learning	Unsupervised ML
<b>Decisioning</b>	
	Decision orchestration
<b>Business model</b>	
Pricing model	Pricing is per transaction and based on volume and complexity.
<b>Fraud prevention partners</b>	
Investors	Seed – Halkin Ventures, Series A – Oyak Group, Series B – Equable Capital
Year-over-year growth rate	Triple digit growth – 500%+
Number of employees	150+
Future developments	Proof of Address, Age Verification, Authentication, and continued document/language expansion. Further information available upon request.
<b>Customers</b>	
Customers reference	Experian, Equifax, Plaid, AMEX, ING, HalkBank, Vodafone, ZIP, Hertz, Reed, Admiral Money, CoinMetro
	<a href="#">View company profile in online database*</a>
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .

# The Generative AI Disruption \ of Fraud & Risk Management is Changing...



...Identity Verification For Your World \



Company		INFORM GmbH	
		INFORM develops software for the optimisation of business processes using Digital Decision Making based on Artificial Intelligence and Operations Research. With RiskShield, INFORM provides an intelligent, multi-channel customer-centric fraud prevention and AML compliance solution with proven reliable, fast, and responsive fraud detection results within milliseconds, optimising efficiencies and minimising losses.	
<b>Background information</b>			
Year founded	1969		
Website	<a href="http://www.inform-software.com">www.inform-software.com</a>		
Target group	<ul style="list-style-type: none"> <li>• Banks/FS</li> <li>• PSP/acquirers</li> <li>• Telecom</li> </ul>		
Supported regions	Europe; US; APAC; Africa; LATAM		
Contact	Tyrone Castelanelli, Product Marketing, <a href="mailto:tyrone.castelanelli@inform-software.com">tyrone.castelanelli@inform-software.com</a>		
Member of industry associations and/or initiatives	ETIS; UN Global Compact Network Germany; BANKINGCLUB; Coalition Against Insurance Fraud (CAIF)		
<b>Core solution</b>			
Core solution/problems the company solves	<ul style="list-style-type: none"> <li>• Fraud and financial crime hub – decision platform</li> <li>• Transaction fraud</li> <li>• Account fraud</li> <li>• AML transaction monitoring</li> <li>• KYC/CDD</li> </ul> <p>With its Product RiskShield, INFORM is a global provider of solutions for AML compliance and fraud prevention, offering a flexible Financial Crime Prevention platform that enables customers to implement customer and transaction behaviour monitoring in compliance with national and international regulations. RiskShield provides a user-friendly interface for configurations, ad-hoc analysis, and alert and case management functionalities. Its platform is fully customisable to meet the specific needs of its business partners, with applications for rule management, case management, reporting, and data integration.</p> <p>As a strategic enterprise financial crime prevention technology provider, INFORM is constantly researching and developing new technologies to enhance the effectiveness of its services. Over the last 25 years, INFORM has built up its expertise in Hybrid AI, and experiences in best practices in fighting financial crime through projects across 25 different countries.</p>		
<b>Technology</b>			
	<ul style="list-style-type: none"> <li>• On-premise</li> <li>• Cloud-enabled</li> <li>• Hybrid</li> </ul>		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Credit check	x		
Compliance check	x		
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Geo-location	x		
3-D Secure 2.0			x
Knowledge-based authentication			x

Intelligence	proprietary capability	third party	both
Abuse list		x	
Financial crime data		x	
Watchlist screening	x		
Information sharing	x		
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	
<b>Methodology</b>			
Machine learning	<ul style="list-style-type: none"> <li>• Rule-based</li> <li>• Supervised ML</li> <li>• Unsupervised ML</li> <li>• Hybrid</li> </ul>		
<b>Decisioning</b>			
	<ul style="list-style-type: none"> <li>• Manual review</li> <li>• Case Management</li> <li>• Decision orchestration</li> </ul>		
<b>Business model</b>			
Pricing model	We offer flexible pricing models including Perpetual, SaaS, and subscription-based models.		
Fraud prevention partners	Netcetera, Huron Consulting Group, Ordina		
Investors	INFORM is a privately-owned company, growing completely organically, with no third-party investors.		
Year-over-year growth rate	20%		
Number of employees	900		
Future developments	At INFORM, we are committed to staying at the forefront of Hybrid AI technology to improve our ability to detect and combat financial crime continuously. Additionally, we place a strong emphasis on enhancing the user experience. In recent years, we have developed and designed a new technology framework with the user in mind. This has led to the release of several products, including RiskShield Case Management (which features enhanced workflow capabilities), RiskShield Machine Learning, and RiskShield Rule Management. These products are complemented by an intuitive user interface, which boosts productivity and streamlines workflows for rule writers, Fraud/AML analysts, investigators, and data scientists. Our development team is also dedicated to enhancing our network visualisation technology as part of our case management solution. This will involve implementing new techniques such as reasoning entity.		
<b>Customers</b>			
Customers reference	More than 250 banks, financial institutions, insurances, and telecommunications companies across Europe, the Americas, Africa, and Australia protect their companies with the vast solution portfolio offered by RiskShield.		
		View company profile in online database*	
		*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .	

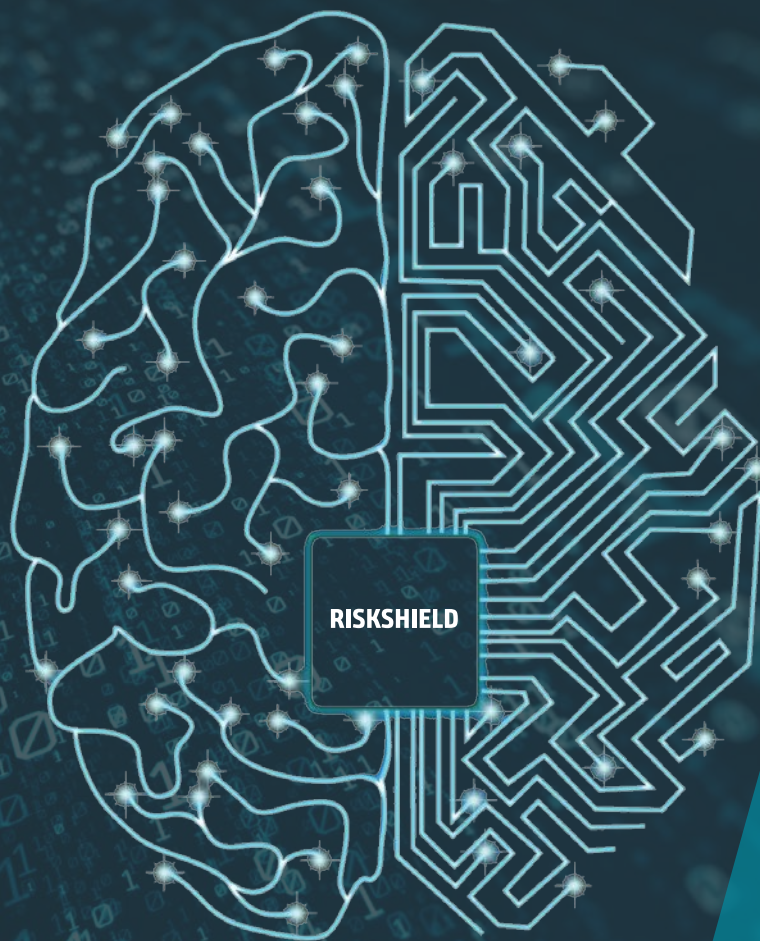
# Fighting Financial Crime with Hybrid AI



RiskShield brings your financial crime prevention strategy to the next level by combining the best Human Intelligence-based AI and Machine Learning technology into one single solution.


**HYBRID**

**AI**



For more information, visit [ml.riskshield.com](http://ml.riskshield.com) and request a copy of our paper, or contact us at [riskshield@inform-software.com](mailto:riskshield@inform-software.com)



Company		NetGuardians	
 <b>NetGuardians</b>		NetGuardians is an award-winning Swiss fintech helping commercial, retail, and private banks worldwide protect more than USD 7 trillion of assets from fraud and financial crime. Headquartered in Switzerland, it has offices in Singapore, Kenya, and Poland.	
<b>Background information</b>			
Year founded	2007		
Website	<a href="http://www.netguardians.ch">www.netguardians.ch</a>		
Target group	Banks/FS		
Supported regions	Europe; Middle East; APAC; Africa; US		
Contact	<a href="mailto:info@netguardians.ch">info@netguardians.ch</a>		
Company's motto	Together We Fight Financial Crime		
<b>Core solution</b>			
Core solution/problems the company solves	<ul style="list-style-type: none"> <li>• Fraud and AML alert handling and decisioning platform/ solution</li> <li>• Transaction fraud</li> <li>• AML transaction monitoring</li> </ul> NetGuardians' Fraud and AML solutions help you accurately prevent fraud and detect suspicious transactions whilst intelligently ensuring operational efficiency. Confidently protect your customers' transactions, maintain frictionless customer journeys, and safeguard your business.		
<b>Technology</b>			
	<ul style="list-style-type: none"> <li>• On-premise</li> <li>• Cloud enabled</li> <li>• 3D AI</li> </ul>		
<b>Data input</b>			
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Behavioural biometrics		x	
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Financial crime data			x
Information sharing			x
<b>Decisioning</b>			
	<ul style="list-style-type: none"> <li>• Case management</li> <li>• Decision orchestration</li> </ul>		
<b>Business model</b>			
Pricing model	More information available upon request		
Fraud prevention partners	Swisscom, Finastra, Mambu, Microsoft, Avaloq		
Investors	Pictet Group, Ace & Company, Swisscom Ventures, Freemont Management		
Year-over-year growth rate	51%		
Number of employees	85		
Future developments	More information available upon request		
<b>Customers</b>			
Customers reference	Pictet, UOB, Lombard Odier, Raiffeisen Luxembourg, Bank of Africa, Swissquote, Zurich Cantonal Bank, tonik, Consolidated Bank of Ghana		
		View company profile in online database*	
		*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .	



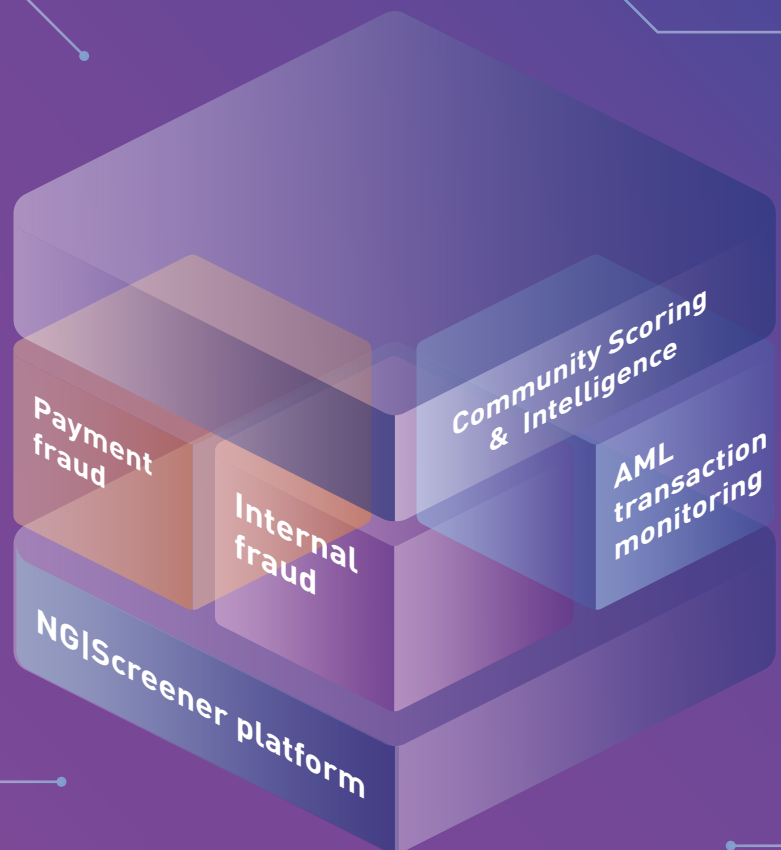


NetGuardians

# Intelligently prevent fraud and detect money laundering risks.

Centralize risk and compliance management utilizing optimized AI models that continually learn. Leverage NetGuardians Community Scoring & Intelligence service for actionable insights to expand your risk signals.

Discover




For more information, please contact us:

[info@netguardians.ch](mailto:info@netguardians.ch) | [www.netguardians.ch](http://www.netguardians.ch)



Switzerland | Singapore | Nairobi | Warsaw

Company		NICE Actimize		
		<p>NICE Actimize is the largest provider of financial crime, risk, and compliance solutions for financial institutions. The company offers real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance products that address payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence, and insider trading. Find us at <a href="http://www.niceactimize.com">www.niceactimize.com</a>.</p>		
<b>Background information</b>				
Year founded	1999			
Website	<a href="http://www.niceactimize.com">www.niceactimize.com</a>			
Target group	<ul style="list-style-type: none"> <li>• Banks/FS</li> <li>• Fintech</li> <li>• Brokers</li> <li>• Crypto exchange/Blockchain and crypto companies</li> <li>• Merchants/Marketplaces (regulated entities)</li> <li>• PSP/acquirers</li> <li>• Telecom</li> </ul>			
Supported regions	Global			
Contact	<a href="mailto:info@niceactimize.com">info@niceactimize.com</a>			
Company's motto	Know More. Risk Less.			
Member of industry associations and/or initiatives	The Knoble			
<b>Core solution</b>				
Core solution/problems the company solves	<ul style="list-style-type: none"> <li>• Fraud and financial crime hub – decisioning platform</li> <li>• Transaction fraud</li> <li>• Account fraud</li> <li>• Financial crime data provider and intelligence</li> <li>• AML transaction monitoring</li> <li>• KYC/CDD</li> <li>• KYC remediation</li> <li>• Digital identity service provider</li> <li>• Identity verification</li> <li>• Authentication</li> </ul> <p>NICE Actimize's FinCrime and compliance solutions leverage the latest AI advances to cut fraud losses and ensure complete AML-KYC compliance, providing FIs with lower false positives rates and better customer experiences.</p>			
<b>Technology</b>				
	<ul style="list-style-type: none"> <li>• On-premise</li> <li>• Cloud-enabled</li> <li>• Native cloud</li> <li>• Hybrid</li> </ul>			
<b>Data input</b>				
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>	
Identity document scanning			x	
Video scanning			x	
Personally Identifiable Information (PII) validation			x	
Small transaction verification			x	
Email verification			x	
Phone verification			x	
Social verification			x	
Credit check	x			
Compliance check			x	

Online authentication	proprietary capability	third party	both
Behavioural biometrics		x	
Physical biometrics		x	
Device fingerprinting			x
Geo-location			x
Remote access detection		x	
Mobile app push		x	
3-D Secure 2.0			x
One-time passwords		x	
Knowledge-based authentication		x	
Intelligence	proprietary capability	third party	both
Abuse list	x		
Financial crime data			x
Sanctions data (sanctions, enforcements, PEP, and adverse media)	x		
Watchlist screening	x		
Address verification		x	
Credit bureau	x		
Information sharing	x		
Data ingestion/third-party data			
Stateless data ingestion and augmentation	X-Sight DataIQ and X-Sight Marketplace partners provide integrated data that is delivered seamlessly within NICE Actimize solutions to fuel analytics and enrich investigations. NICE Actimize's analytics solutions ingest transactional and non-transactional data.		
Methodology			
Machine learning	<ul style="list-style-type: none"> <li>• Rule-based</li> <li>• Supervised ML</li> <li>• Unsupervised ML</li> <li>• Hybrid</li> </ul>		
Decisioning			
	<ul style="list-style-type: none"> <li>• Manual review</li> <li>• Case management</li> <li>• Decision orchestration</li> </ul>		
Business model			
Pricing model	Depends on the type of client deployment. NICE Actimize offers Perpetual, SaaS, and Term licences.		
Fraud prevention partners	NICE Actimize has 100s of partners offering a wide variety of complementary solutions.		
Investors	NICE Actimize is a subsidiary of NICE. NICE is a public company NASDAQ:NICE		
Year-over-year growth rate	NICE's revenue across all lines of business, including NICE Actimize, grew 13%.		
Number of employees	NICE has 8000 employees globally across all lines of business.		
Future developments	In 2023, NICE Actimize announced the launch of SAM-10 (Transaction Monitoring), Mule Defense, and ActOne10 (Case Management).		
Customers			
Customers reference	NICE Actimize does not publish client information.		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		




# Detect with precision


using a multilayered approach to transaction monitoring



No one detection tool is infallible. To detect all suspicious activity, your organisation needs a multilayered approach that combines rules, advanced analytics, and network risk analysis to maximise effectiveness. One that turns data into intelligence and continuously optimises for accurate decisions all the time.

→ Comply with Confidence

Company		Ping Identity	
		<p>Ping Identity is the Intelligent Identity solution for the enterprise. We provide flexible identity solutions that accelerate digital business initiatives, delight customers, and secure the enterprise through multi-factor authentication, single sign-on, access management, fraud management, intelligent API security, directory, and data governance capabilities.</p>	
<b>Background information</b>			
Year founded	2002		
Website	<a href="http://www.pingidentity.com">www.pingidentity.com</a>		
Target group	<ul style="list-style-type: none"> <li>• Merchants/Marketplaces</li> <li>• Banks/FS</li> </ul>		
Supported regions	Global		
Contact	Divya Handa		
Member of industry association and/or initiatives	MRC, FIDO		
<b>Core solution</b>			
Core solution/problems the company solves	<ul style="list-style-type: none"> <li>• Fraud and financial crime hub – decisioning platform</li> <li>• Account fraud</li> <li>• Digital identity service provider</li> <li>• Identity verification</li> <li>• Authentication</li> </ul> <p>Ping Identity's fraud management solutions combine fraud and risk detection, decisioning, ID verification, authentication, and orchestration tools to create a complete fraud detection and mitigation solution.</p>		
<b>Technology</b>			
	<p>All, depending on solution:</p> <ul style="list-style-type: none"> <li>• On-premise</li> <li>• Cloud enabled</li> <li>• Native cloud</li> <li>• Hybrid</li> </ul>		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Identity document scanning	x		
Video scanning	x		
Personally Identifiable Information (PII) validation			x
Email verification	x		
Phone verification	x		
Social verification		x	
Credit check		x	
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Behavioural biometrics	x		
Physical biometrics	x		
Device fingerprinting	x		
Geo-location	x		
Remote access detection	x		
Mobile app push	x		
Hardware token	x		
One-time passwords	x		
Knowledge-based authentication	x		

Intelligence	proprietary capability	third party	both
Address verification	x		
Credit bureau		x	
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	
<b>Methodology</b>			
Machine learning	<ul style="list-style-type: none"> <li>• Rule-based</li> <li>• Supervised ML</li> <li>• Unsupervised ML</li> <li>• Hybrid</li> </ul>		
<b>Decisioning</b>			
	Decision orchestration		
<b>Business model</b>			
Pricing model	Pricing will depend on the collection of solutions that customers require to meet their use case.		
Fraud prevention partners	See the full list of integrations and partners <a href="#">here</a>		
Investors	We are owned by Thoma Bravo.		
Year over year growth rate	23%		
Number of employees	1,232		
Future developments	<p>Ping is unifying our existing fraud, risk, and orchestration services to deliver a comprehensive threat mitigation solution. The solution will initially target identity buyers, desiring to protect mainly against Account Takeover and New Account Fraud. Ping will deliver an end-to-end, frictionless, risk management solution for CIAM &amp; WIAM use cases. The solution will differ from other vendor solutions by providing:</p> <ol style="list-style-type: none"> <li>1. a well-integrated set of flows with risk and fraud capabilities that deliver detection and insights for broad sets of attack vectors and risk signals</li> <li>2. options for mitigating those threats with services such as MFA, authorisation, and verification</li> <li>3. insights from single alert level to system level (new type of attack detected) to accelerate the ability to respond</li> <li>4. these capabilities with the 3rd-Party risk and fraud providers via PingOne DaVinci</li> </ol>		
<b>Customers</b>			
Customers reference	<a href="https://www.pingidentity.com/en/customer-stories.html">https://www.pingidentity.com/en/customer-stories.html</a>		
	View company profile in online database* 		
	<p>*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a>.</p>		





# Know Your Customers

The Power of Digital Identity for Financial Services



Transferring Funds to Checking

Transfer Complete

Whether welcoming a brand new customer or issuing a new loan to an existing client, financial institutions need absolute certainty regarding customers' identities. When financial institutions can accurately and quickly identify customers at high-risk points across the customer journey, they have the opportunity to offer better digital services and expand digital ecosystems while improving security and cutting losses at the same time.


## With our fraud prevention report, you can:


- Identify key identity-related risks in financial services
- Learn the role of identity proofing and verification throughout the customer lifecycle
- See how identity proofing works with access management and fraud detection tools to deliver better customer experiences
- View top identity proofing use cases and outcomes
- Unlock the future of digital identity utilizing emerging technologies that will transform the industry


[Watch this webinar for more details](#)

[pingidentity.com](https://pingidentity.com)



Company	Refine Intelligence
	<p>Refine Intelligence introduces a new paradigm for fighting financial crime by ‘catching the good guys.’ We enable banks to regain their ‘superpower’ of understanding customers’ life events that create changes in their financial activity. Our AML technology uses AI to automatically identify the life story behind each transaction monitoring alert.</p>
<b>Background information</b>	
Year founded Website Target group Supported regions Contact Company’s motto Member of industry associations and/ or initiatives	2022 <a href="https://www.refineintelligence.com/">https://www.refineintelligence.com/</a> Banks/FS Global <a href="mailto:sales@refineintel.com">sales@refineintel.com</a> Catching the Good Guys ACFCS, ACAMS
<b>Core solution</b>	
Core solution/problems the company solves	Financial crime data provider and intelligence Almost every alert an AML team investigates ends up being a totally legitimate customer activity. Refine spots the real-life story behind those alerts, cutting 90% of investigation time.
<b>Technology</b>	
	Cloud enabled
<b>Data input</b>	
	<p>The Refine intelligence platform allows financial institutions to quickly clear away AML or Scam alerts that were actually triggered by legitimate customer activity. There are two methods to achieve that:</p> <p><b>Digital Outreach</b> allows a bank to reach out to customers automatically and collect their explanation to flagged anomalies in their account. The response is received within minutes. It is used to replace branch or call center work around AML or CDD/EDD.</p> <p><b>Life Story Analytics</b> is an AI model trained to automatically detect the legitimate life story behind an anomaly. It trains on a unique, proprietary dataset of validated customer explanations for anomalies in their account. It provides clear evidence for the detected life story and is used to significantly cut AML or Scam Investigation time.</p>
<b>Methodology</b>	
Machine learning	Supervised ML
<b>Decisioning</b>	
	Decision orchestration
<b>Business model</b>	
Pricing model Fraud prevention partners Investors Year-over-year growth rate Number of employees Future developments	Annual fee based on customer base tier Information available upon request. Glilot Ventures, SYN Ventures, GroundUp, Ori Eisen Confidential 10 Auto-hibernation using Life Story Analytics
<b>Customers</b>	
Customers reference	Top 50 US Bank + POCs implemented with additional Top 10 Banks
<div style="text-align: right; background-color: #c00000; color: white; padding: 5px;">View company profile in online database* </div>	
<p>*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a>.</p>	

Company		ThreatFabric	
		<p>ThreatFabric utilises web and mobile threat intelligence to offer advanced online fraud detection solutions for the financial industry. Their cutting-edge technologies, such as behavioural analytics, device fingerprinting, and adaptive fraud indicators provide businesses with real-time fraud prevention and detection to ensure safe online experiences.</p>	
<b>Background information</b>			
Year founded	2015		
Website	<a href="https://www.threatfabric.com/">https://www.threatfabric.com/</a>		
Target group	Financial institutions and ecommerce		
Supported regions	ThreatFabric supports banks, financial institutions, and law enforcement across the globe with markets in Europe, the UK, and Asia.		
Contact	<a href="mailto:han.sahin@threatfabric.com">han.sahin@threatfabric.com</a>		
Company's motto	Peace of mind for you and your customers.		
<b>Core solution</b>			
Core solution/problems the company solves	<ul style="list-style-type: none"> <li>• Transaction fraud</li> <li>• Account fraud</li> <li>• Financial crime data provider and intelligence</li> </ul> <p>ThreatFabric offers a SaaS solution to the financial sector, enabling fraud detection across web and mobile channels with features like threat intel, malware threat detection, behavioural analytics, and advanced device fingerprinting. We have a web and mobile SDK and online portal that handles the early fraud indicators inside online payment journeys. Detecting fraud prior to the transaction is key in a world of instant payments.</p>		
<b>Data input</b>			
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Behavioural biometrics	x		
Device fingerprinting	x		
Geo-location	x		
Remote access detection	x		
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Abuse list	x		
Financial crime data	x		
Information sharing	x		
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	
<b>Methodology</b>			
Machine learning	Supervised ML		

Business model	
Fraud prevention partners	Trapets, Hawk AI, Fox-IT
Investors	Lead investors Motive Ventures, ABN AMRO Bank Ventures, with participation from 10xFounders and 14Peaks capital.
Year-over-year growth rate	For more info regarding Year-over-year growth rate you can reach us at <a href="mailto:han.sahin@threatfabric.com">han.sahin@threatfabric.com</a> .
Number of employees	Approx. 50
Future developments	Behaviour based location intelligence, AI driven threat modelling as part of behavioural biometrics.
Customers	
Customers reference	ABN AMRO Bank, Rabobank, iDEAL, Natwest, Barclays, BNP Paribas, CBA, Metro bank, ANZ, Erste Group
	View company profile in online database* 
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .



THREAT  
FABRIC



Accurate realtime fraud detection and rich device context for transaction monitoring



Based on industry leading threat intel to detect all modern online payment fraud



APP fraud detection using early fraud risk indicators and behavioural analysis



Continuous Authentication using behavioural analysis



Additional device context for customer support teams

Peace of mind  
for you and  
your customers

More information or demo:



[info@threatfabric.com](mailto:info@threatfabric.com)



[www.threatfabric.com](http://www.threatfabric.com)


## Detect fraud

Authorized Push Payment (APP) fraud  
Account Takeover (ATO) fraud  
Account Opening (AO) fraud  
Device Takeover (DTO) fraud **NEW**

User?



Fraudster?

Company		Trulioo	
		<p>Trulioo is the identity platform global businesses turn to for growth, innovation, and compliance. The platform helps companies achieve regulatory compliance, reduce risk, and expand their businesses by enabling verification of more than 5 billion people and 300 million businesses across 195 countries.</p>	
<b>Background information</b>			
Year founded	2011		
Website	<a href="http://www.trulioo.com">www.trulioo.com</a>		
Target group	<ul style="list-style-type: none"> <li>• Banks/FS</li> <li>• Fintech</li> <li>• Brokers</li> <li>• Crypto exchanges</li> <li>• Marketplaces/Merchants</li> <li>• PSPs</li> </ul>		
Supported regions	Global		
Contact	<a href="mailto:info@trulioo.com">info@trulioo.com</a>		
Company's motto	The World's Identity Platform		
Member of industry associations and/or initiatives	Council of Canadian Innovators, BC Tech Association, Business Information Industry Association, Merchant Risk Council, Women in Identity, TAP Network		
<b>Core solution</b>			
Core solution/problems the company solves	<p>Identity Verification Platform for Businesses and Individuals</p> <p>Trulioo is the only global identity verification platform providing KYC, KYB, document verification, and fraud detection &amp; deterrence solutions, through one contract, orchestrated, and integrated into bespoke configurations.</p>		
<b>Technology</b>			
	Hybrid		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Identity document scanning	x		
Personally Identifiable Information (PII) validation	x		
Email verification	x		
Phone verification	x		
Compliance check	x		
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Physical biometrics	x		
Geo-location	x		
One-time passwords		x	
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Abuse list	x		
Financial crime data	x		
Sanctions data (sanctions, enforcements, PEP, and adverse media)	x		
Watchlist screening	x		
Address verification	x		
Credit bureau	x		
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	



<b>Methodology</b>	
Machine learning	Hybrid (depending on service)
<b>Decisioning</b>	
	Decision orchestration
<b>Business model</b>	
Pricing model	Per transaction
Fraud prevention partners	Information available upon request
Investors	TCV, Blumberg Capital, American Express, Citi Ventures, Santander, Goldman Sachs
Year-over-year growth rate	Information available upon request
Number of employees	425+
Future developments	Information available upon request
<b>Customers</b>	
Customers reference	KOHO Financial, STACK, Bitbuy, Nium, Webull, IG Group, World Remit, and additional available upon request.
	<a href="#">View company profile in online database*</a>
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .



# Onboard Your Customers With Certainty

Leverage the Trulioo global identity platform for fast, secure onboarding while keeping fraudsters at the gate

1

Strengthen fraud prevention with customizable identity verification workflows that adapt to different risk profiles

2

Grow your customer base by verifying customers around the world with a global network of more than 450 data sources across 195 countries

3

Enhance customer trust and safety with layered verification that paves the way for smooth user experiences

Trulioo



Request a demo today



## Don't Miss the Opportunity of Being Part of Large-Scale Payments Industry Overviews

Once a year, The Paypers releases six large-scale industry overviews covering the latest trends, developments, disruptive innovations, and challenges that define the global online and mobile payments, e-invoicing, B2B payments, ecommerce, and web fraud prevention and digital identity space. Industry consultants, policy makers, service providers, and merchants from all over the world share their views and expertise on different key topics within the industry. Listings and advertorial options are also part of the guides for the purpose of ensuring effective company exposure at a global level.



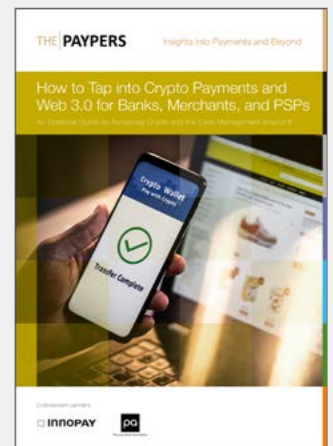
Fraud Prevention in Ecommerce Report 2022-2023



Digital Onboarding and KYC 2022 – The Essentials of Identity Verification



Cross-Border Payments and Ecommerce Report 2022-2023



Crypto Payments and Web 3.0 for Banks, Merchants, and PSPs Report

For the latest edition, please check the [Reports section](#)

