SYNECTICS CONNECT
SUMMER 2019 / ISSUE 9

SYNECTICS
SOLUTIONS

CONNECT

CONNECTING BUSINESSES THROUGH KNOWLEDGE

SYNECTICS DIGITAL ID CONFERENCE – LONDON SEPT 2019

The consequences for fraud and financial crime in an age of digital identity - book your place today.

EMAIL RISK PROFILING

emailage

Why is the email address so powerful in the fight against fraud?

SHARING INTELLIGENCE

EQUIFAX

Equifax explores how companies are moving toward SaaS and cloud based platforms to make them more agile and change resilient.

PLATFORMIFICATION

Find out why creating a single customer view of financial crime risk management is an essential component in securing the future for your organisation...

CONTENTS

3
Message from our Business Development Manager

"In the social jungle of human existence, there is no feeling of being alive without a sense of identity." – Erik Erikson.

4

Platformification

Connect explores the importance of creating a single customer view of risk and developing an effective Financial Crime Risk Management platform fit for tomorrow.

6
The case for a single customer view of risk

Establishing the need for a more holistic platform to address Financial Crime Risk Management

7-8
Managing the increasing burden of Regulatory Compliance

What challenges do organisations face when adhering to regulatory obligations and what can be done to help reduce overall customer risk and help improve their operational resilience?

9
Why is the humble email address a key component in the fight against fraud?

emailage

On the surface, an email address only appears to provide a limited source of data, but underneath it has potential to unlock a whole new world.

10

Credit Declines –

Should not be ignored when it comes to their potential to improve fraud indicators in your investigation process.

12
The implications for fraud, financial crime and customer authentication in an age of digital identity

Synectics is hosting a major conference to explore the ramifications for fraud and financial crime in an age of digital identity and authentication. Book your place today!

14

BOOK YOUR PLACE NOW!

Fraud and Financial Crime in the age of Digital Identity

SYNECTICS SOLUTIONS CONFERENCE

London, September 26th 2019

15
esure Named Celent Model Insurer for Precision Success

esure

esure wins a prestigious award for successfully implementing Precision.

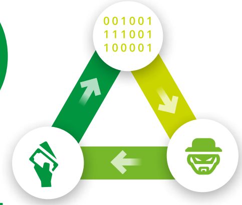
EQUIFAX

16
Equifax explores how companies are moving toward SaaS and cloud based platforms to give them more agility and change resilience.

18
Who are the real victims of misuse of accounts in the UK and where are they based?

Who is most affected by the misuse of accounts and is the demographic and geographic evidence different than we may think?

20

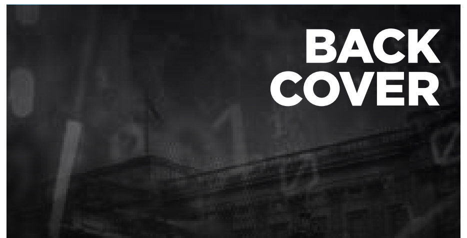


Collaboration is key when dealing with criminals using the dark web as part of their 'cyber crime triangle' to cash out.

Find out more...

22
Fraud insights and trends reports

The results of our latest fraud trends analysis are now in!



BACK COVER

Our Queen's Award for Enterprise – Innovation 2019

Synectics is delighted to win the Queen's Award for Enterprise – Innovation 2019.

Look out for our clickable links...

If you are using the Digital version of Connect then look out for our clickable links, these links will give you access to more information relating to the article including thought leadership and research.

Identity and the jungle of human existence

> **"Be yourself; everyone else is already taken."**
> *Oscar Wilde.*

MESSAGE FROM OUR BUSINESS DEVELOPMENT DIRECTOR, RICHARD WOOD

"In the social jungle of human existence, there is no feeling of being alive without a sense of identity." – Erik Erikson.

Computers are well on their way to replace our own cerebral navigation capacity, such as when we use Google maps, and to replace some of our memories that are more reliably stored as images and videos on our smartphones. The algorithms in these machines are also getting smarter, faster and cheaper than the neurons in our central nervous systems that collect sensory input to support decisions about identity.

These algorithms are being developed, refined and reprogrammed for the digital identity age in the UK. As digital identities authenticating people in the UK becomes more widespread, the resultant impact on customer interactions, their journey with your business, and the impact on fraud and financial crime will be significant. Successfully delivering an electronic method of authenticating people can offer intelligent advantages when combatting the scourge of fraud and financial crime that has plagued many financial services companies and government agencies for many years.

Understanding the latest developments that are underway in making this opportunity a reality will be essential to all those tasked with helping to ensure their organisations are prepared for the adoption of E-ID.

With this in mind, our September conference will bring together delegates from across the financial landscape to focus on digital ID in the heart of London. This will include keynote speakers who have a wealth of experience and expertise in the area of fraud and financial crime.

We are also delighted to announce that Synectics Solutions has received a royal seal of approval with a Queen's Award for Enterprise – Innovation. The Queen's Awards, which are the highest official UK accolade for British businesses, aims to promote excellence and drive economic growth. The Innovation category awards companies that go above and beyond in their area of expertise, and is designed for those offering unique innovations.

Identity and our momentum to prioritise and expedite genuine customers as they interact with our clients will be a key driver of our future innovations.

"Be yourself; everyone else is already taken." – Oscar Wilde.

PLATFORMIFICATION

Is it the Holy Grail for FCRM?

Harmonising disparate data models and departmental needs into one solution to create a truly effective Financial Crime Risk Management (FCRM) platform has long been the desire of financial services organisations.

Customers and investors of financial services companies are increasingly becoming aware of those organisations that repeatedly fall foul of financial crime, cyber breach or legal disputes with regulators.

Such is the problem that regulators, such as the Financial Conduct Authority (FCA) in its 2019/20 business plan, are increasingly requiring organisations to show that their intelligence is capable of being shared across their organisations.

They are also starting to call out the need for these systems to go beyond slow, cumbersome manual processes to become more automated. This is to aid the reduction in costly post-event remediation activities that often fail to recover funds once acts of financial crime have been perpetrated. Ultimately threats from employee attacks, anti money laundering (AML) tactics – allied to the added complication of a borderless banking environment – has meant that financial services organisations are increasingly realising that centralised FCRM platforms are becoming an essential component for the future protection of their organisation.

An enterprise-wide approach to FCRM that offers a single customer view of risk can help to ensure a strategy capable of avoiding the pitfalls of working in silos. Additional benefits of this also enables streamlining of processes, reduced costs, automation of routine tasks, reduction of regulatory risk, and a better ability to defend the entire organisation against a whole raft of attacks.

However, the deployment of an enterprise wide FCRM platform is something that has eluded financial services companies to date.

Many organisations report having a multitude of different systems across departments (up to 30 in certain large banks) and different product lines that all have completely different data models, and procedures. Operating in this way means that organisations are not only missing the opportunity to share intelligence effectively across their organisation, but are also duplicating tasks, and increasing the risk of falling victim to a variety of costly criminal activities.

Many organisations point to the cost of aligning their FCRM solutions across the organisation. Lack of budget / investment, poor quality data, lack of common standards, and relevant expertise, are all things that seem to prevent addressing the issue. However, what senior decision makers are failing to realise by withholding investment is that they are missing the opportunity to develop a resilient enterprise through a more coherent approach to financial crime risk mitigation.

Investing in the deployment of an organisation-wide FCRM solution allows senior management to place much more effective controls across the organisation so that it can withstand the full range of fraud, financial crime and compliance risks, disruptions and requirements of today. Some of the more granular benefits of deploying an organisation-wide FCRM platform also includes:

- Reducing the cost of fraud / AML investigations
- Less reliance on repetitive manual processes
- Reduction in remediation activities
- Increased speed of customer boarding
- Competent management of regulatory controls
- Improved ability to bring new products to market faster
- Automatic treatment strategy risk alerts

SOME OF THE MORE **GRANULAR BENEFITS** OF DEPLOYING AN ORGANISATION-WIDE FCRM PLATFORM ALSO INCLUDES:

REDUCING FALSE POSITIVES AND THE COST OF FRAUD / AML INVESTIGATIONS

LESS RELIANCE ON COSTLY REPETITIVE MANUAL PROCESSES

INCREASED SPEED OF CUSTOMER BOARDING

COMPETENT MANAGEMENT OF (AND ADHERENCE TO) REGULATORY CONTROLS

IMPROVED ABILITY TO BRING NEW **PRODUCTS TO MARKET FASTER**

The benefits of having a single customer view of risk, also means that organisations can benefit from being more competitive (thanks to the huge efficiency gains inherent in such an approach) as well as having an enhanced brand value and resilient share price.

A quick look at some examples of failing approaches to FCRM resulted in UK banks suffering over £500 Million losses to fraud in 2018 alone (according to UK finance), not to mention examples of fines for breaches in AML regulations for some of these organisations including; Deutsche Bank, BNP Paribas and Standard Chartered, all averaging around £500 Million to £1 Billion pound mark.

So the case for taking advantage of a better use of technology to improve FCRM and create a more coherent view of financial risk couldn't be clearer.

One of the things that has held many organisations back is the desire to marry old legacy systems with new, more agile, platforms. This tactic has not always yielded great results as projects have stalled due to the inability of old systems to supply the speed, accuracy, and agility to process and analyse the volume of online transactions required.

An approach now being more actively considered is to deploy a cloud based FCRM platform that can be accessed across the organisation without the need to deploy expensive hardware. This also often mitigates the need to recruit automation expertise in-house, as vendors often supply this resource and functionality.

An additional point to consider is the power of exploiting wider networks when deploying FCRM platforms. The power of networks has to be one of the greatest advances in organisation effectiveness since the Internet enabled much wider and faster sharing of data.

Platforms that can enable organisations to access wider networks means better leverage of sector-wide intelligence, as well as intelligence from other sectors to exponentially improve the ability to detect, predict and act on anomalies that threaten the organisation's assets.

An organisation that exploits this networked intelligence, such as using consortium data or shared government intelligence sources, has much greater ability to create a defensive posture that will deter the most ardent of financial criminals.

Examples of the value of this type of networked value are not difficult to come by with databases such as National SIRA and CIFAS demonstrating year after year their efficacy in helping to prevent and detect billions of pounds in attempted fraud for those companies with the foresight to invest in these communities.

Of course large organisations have a multitude of requirements across the full panoply of risk mitigation, and so it becomes important for any platform to offer a pick and mix approach to the multi-layered functionality and data enrichment on offer – so as to avoid over engineering solutions or adding unnecessary cost in some areas of the organisation without depriving other departments with more complex needs.

Platformification - Continued...

The case for a single customer view of risk

Establishing the need for a more holistic platform to address Financial Crime Risk Management

UK FINANCE ECONOMIC CRIME ACADEMY

UK FINANCE / SYNECTICS ECONOMIC CRIME ACADEMY WEBINAR ATTENDEES AGREE THE NEED FOR A SINGLE CUSTOMER VIEW OF FINANCIAL RISK

One approach that many organisations are now taking to address the growing needs in this area is the establishment of a more holistic system that is sensitive to the requirements of each area of their business, but also capitalises on the opportunities to remove duplication of effort and expensive, inaccurate manual processes where possible.

RESULTS OF SYNECTICS / UK FINANCE ECONOMIC CRIME ACADEMY REVIEW OF CREATING A SINGLE CUSTOMER VIEW OF RISK

During a recent webinar hosted by UK Finance, Synectics posed some questions to UK Finance members about their struggles in establishing a ‘single customer view’ (SCV) of financial risk when attempting to create a centralised FCRM. A huge majority (71.2%) of registrants stated that they had not been successful in establishing an SCV but thought that the concept would be hugely beneficial to their organisation.

The main drivers for exploring this appeared to be cost reduction, but a significant number also saw that having a unified platform that is accessed by multiple teams for the purposes of fraud prevention, financial crime detection and regulatory compliance purposes will be essential to address the rising cost of protecting the organisation and remaining compliant .

Recent research by McKinsey and Thomson Reuters (in their 2018 compliance reports) suggests that as much as 0.4% of revenue is spent on financial crime prevention and compliance work – which in a mid to large sized financial institution is a colossal sum that could be as much a £1Billion a year. Allied to this cost is the increasing burden of retaining large numbers of staff to operate costly manual processes and the increasingly large fines meted out to those organisations who are not keeping up pace with frequently changing regulatory obligations.

AVERAGE FINES FOR REGULATORY BREACHES ARE REACHING INTO THE BILLIONS FOR MID TO LARGE SIZED BANKS AS REGULATORS GET TOUGHER IN AREAS SUCH AS AML

Significant savings to this burden can and will be made by those organisations who embrace the potential for creating a unified FCRM platform and start to build an intelligent, accurate and efficient financial intelligence unit to address these problems.

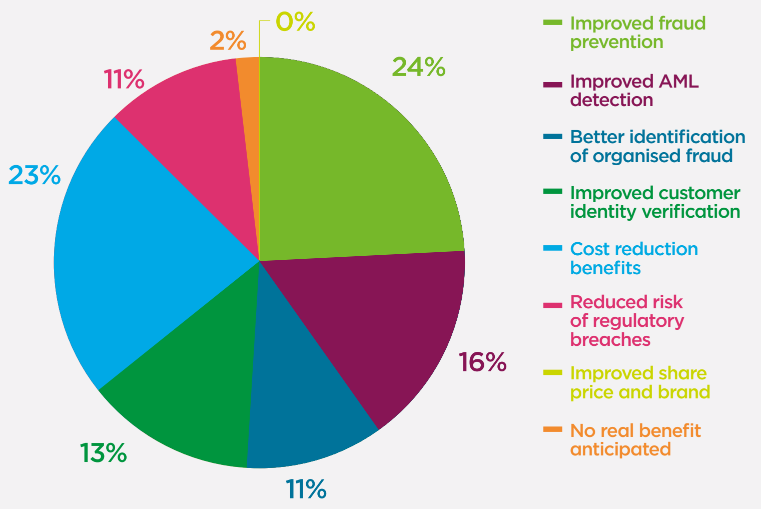
What our UK Finance webinar results highlighted:

SYNECTICS SOLUTIONS UK FINANCE

Has your organisation been able to develop a ‘single customer view’ of your customer base for risk mitigation purposes?

28.8% - YES **71.2%** - NO

Where do you see the biggest opportunities deploying a single customer view of risk?



24.2% of attendees felt that: **creating a single customer view of risk would improve fraud prevention**

23.2% of attendees said that: **deploying a single customer view of risk would help to reduce costs**

OUR UK FINANCE WEBINARS SO FAR:

Webinar #1 Addressing the growing threat of impersonation fraud in financial services
www.synectics-solutions.com/our-thinking/details/webinar-addressing-the-growing-threat-of-impersonation-fraud-in-financial-services

Webinar #2 Collaborative data & predictive analytics in the fight against fraud & financial crime
www.synectics-solutions.com/our-thinking/details/collaborative-data-predictive-analytics-fight-fraud-financial-crime

Webinar #3 Creating a single customer view to transform fraud prevention & risk profiling
www.synectics-solutions.com/our-thinking/details/uk-finance-webinar-3

Managing the Increasing Burden of

REGULATORY COMPLIANCE

Regulatory compliance is a huge and costly undertaking for any institution operating in a regulated environment. The Financial Conduct Authority (FCA) estimates that over £650 million is spent on staff costs alone per year.

Customers want to be reassured that the regulated services they are using are fully compliant and that processes and procedures are designed in a way to not only protect them from the risk of financial loss but to also ensure the service they receive is of high quality and does not unduly impact their interactions.

These businesses must, therefore, conduct a range of different checks around their customer acquisitions and existing portfolios that include regular address and identity verification, due diligence around politically exposed persons and sanction screening against consumer and corporate based entities.

With additional and ever-increasing pressures from financial regulators, companies are facing an increasing challenge when it comes to completing these checks and demonstrating compliance.

CONTINUED >

REGULATIONS & CHALLENGES

What are some of the key regulations and compliance challenges companies face in an ever-evolving financial landscape?

REGULATIONS

ANTI MONEY LAUNDERING

As you are probably aware, the Fifth Money Laundering Directive was passed in January 2019, bringing with it a series of amendments in regulation for banks and financial institutions.

One of the key requirements is the need for enhanced due diligence for transactions from high risk countries where the customer is not always physically present and regulating virtual currencies and pre-paid cards to prevent terrorist financing. Creating a centralised Financial Crime Risk Management (FCRM) platform could be essential in protecting your organisation against these threats – ensuring that stringent checks are made on customers from overseas, enabling you to reduce manual processes, improve the ability for continuous monitoring of customers and reduce working in silos.

ENHANCED DUE DILIGENCE

Verifying and authenticating the identity of your customer and managing ongoing risk, whilst ensuring your business is fully compliant with a variety of FCA and PRA guidelines can take up considerable time and resource.

As you know, manual checks are often time consuming, API integration isn't seamless and there are often delays in verification, leading to poor customer experience but also opening up to potentially being seen as non-compliant.

Ongoing monitoring and automated identity verification through a FCRM platform could enable your business to significantly reduce the cost of compliance without compromising your customer boarding processes/life term.

GDPR / DATA ACCURACY

GDPR has more than likely already impacted significantly on your organisation's time and resources to ensure you comply with the regulations.

You may find that an individual's data is stored in a variety of locations across your company, so finding it, correcting it, erasing it and ensuring its accuracy is often a manual and tedious process/life term.

Creating a centralised platform can help your business to avoid working in silos, reduce the time spent on data gathering and resource heavy manual processes but improve your ability to capture accurate, timely and relevant data from your customers that complies.

TOP 5 REGULATORY CHALLENGES

1. LACK OF INNOVATION

Companies are some way behind complying with AML regulations in comparison with counter fraud regulations due to a reliance on legacy systems and slow processes. Deploying an FCRM platform which uses automated systems can enable businesses to catch up and benefit from innovative solutions which can significantly reduce the cost of delivering a much more rapid and comprehensive single customer view of risk.

2. FINANCIAL CRIME AND COUNTER TERRORISM

A wave of regulatory, legislative and legal reforms have come into force around financial crime and counter terrorism. Many companies still adopt traditional practices which aren't conducive to collaboration or intelligence sharing which is high on the regulator's agenda in the forthcoming year.

3. SCALE AND COST OF COMPLYING

Financial organisations spend vast amounts of time and resource ensuring compliance with numerous regulations but it's unsustainable to keep investing in these resources. The Financial Conduct Authority (FCA) estimates the financial services industry is spending over £650 million annually in staff time to combat financial crime. IT costs can be reduced by using a cloud-based platform that can be used across an organisation without the need to utilise expensive and hard to maintain hardware. Other automated systems can increase efficiencies and reduce the reliance on manual processes.

4. MOVING TO A RISK-BASED APPROACH

Is your risk-based approach compliant? An effective risk-based approach to managing financial crime effectively and robustly is a challenge due to the constant shift in regulatory messages. Changes in regulations can become more difficult for companies to adhere to because of these changing priorities.

5. OPERATIONAL RESILIENCE

As the geo-political landscape evolves, new regulations have been introduced with a regulatory focus on consumers and customer treatment.

Old methods of working do not support operational resilience models and associated risks. A potential solution for companies is to implement more agile cost-effective platforms which will support organisation-wide operational resilience models.

To find out how to incorporate email data into your fraud solution, please call your Synectics Solutions Business Development Manager on: **0333 234 3418.**

Why is the email address a key component in the fight against fraud?

An email address can open up a whole world of data.

On the surface an email address only appears to provide a limited source of information and data but underneath it has the potential to unlock a whole new world in fraud prevention and detection.

Nowadays, the majority of people have individual email accounts and use emails as one of their main communication channels so personal email addresses are an easy target for fraudsters to access and misuse and help them carry out their intended criminal activities.

Using an email address that doesn't exist, comes from a high-risk originating country or has been associated with previous fraudulent transactions could be a sign of illegal activity.

But there's a rich vein of data that can be extracted from an email address which can link to IP addresses, domain names, phone numbers and much more which can be crucial in identifying fraudulent activity and stopping a potential fraudster in their tracks.

Companies are now becoming much wiser to the importance of the email address in their risk management and prevention processes.

They are tightening up on email misuse by working with email risk specialists to identify email fraud trends, provide real-time intelligence and being part of global intelligence hubs to help determine whether transactions are fraudulent or legitimate.

We spoke to Emailage – a company which specialises in email risk profiling and uses the email address as a platform to combat fraud. **Emailage is now integrated into the SIRA fraud prevention and detection product from Synectics Solutions.**

emailage

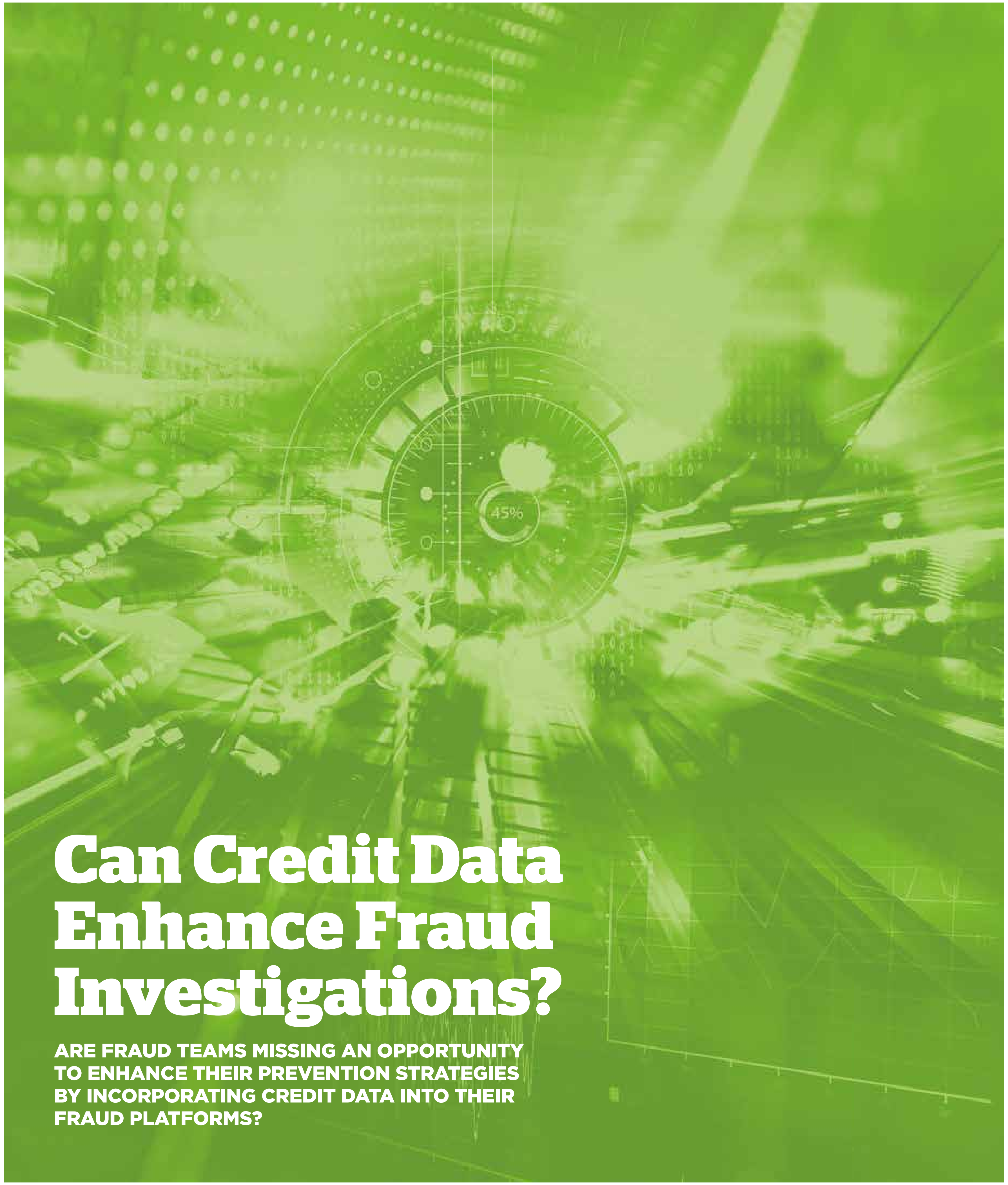
KEY BENEFITS

- Accurate identification of high fraud risk applications
- Reduction in manual review volumes
- Increased acceptance rates using low risk signals

An individual's email address is by far the most robust and reliable global Unique Identifier in the digital era. Emailage has built the world's largest repository of email addresses and their associated behaviour, which allows our clients to access real-time, dynamic fraud risk scoring, whilst sharing intelligence of criminal activity with hundreds of leading brands across the globe. By looking at the email address and its connections to other data elements held in the Emailage network (IP address, Name, Address, Phone number), Emailage can apply their proprietary scoring algorithms to provide a highly accurate risk score. They provide this service to some of the largest global banking and financial services companies, helping them to make better real-time decisions by enabling access to a vast network of digital behavioural data. It is this large pool of global dynamic network data combined with their industry and company level machine learning which makes the product an invaluable tool in the fight against fraud.

Jonathan Knott, EMEA Financial Services Sales Director, said "Emailage has had great success in the Financial Services sector ever since the business inception, working with some of the largest global banks, lenders and card issuers. A typical email address comes with a lot of history and data attached, which our clients find incredibly powerful for both stopping high risk applications as well as helping in the identification of good customers."

To find out more about Emailage, visit: **www.emailage.com/industries/financial**



Can Credit Data Enhance Fraud Investigations?

ARE FRAUD TEAMS MISSING AN OPPORTUNITY TO ENHANCE THEIR PREVENTION STRATEGIES BY INCORPORATING CREDIT DATA INTO THEIR FRAUD PLATFORMS?

Many organisations tasked with preventing fraud have a variety of intelligence at their disposal which can help to supplement their intelligence to spot fraud. However, sometimes important gains can be made in the fight against fraud by taking a look at intelligence sources that may, at first glance, not necessarily be obvious in terms of their efficacy for submitting into a fraud solution.

In this respect, credit checks are often done way earlier in the onboarding journey, before applications get to be reviewed for potential fraud, however, research conducted by Synectics shows that utilising Credit Decline (CD) data in the intelligence mix can often yield significant gains when identifying or preventing fraud.

Synectics FCI team recently carried out a study to understand these benefits more clearly by working with a number of SIRA clients to take some CD data and then analysing that against the National SIRA data base to measure the uplift in fraud identification against known adverse cases.

THE RESULTS WERE IMPRESSIVE TO SAY THE LEAST

3.7 million

Credit Decline records contribute to setting

29k records to adverse

£33.6 million

of potential savings

Benefit to

62

Finance and Insurance members

Credit scoring processes are obviously designed to decline applicants that have stability issues that don't align with a company's specific credit acceptance policy. However, by its nature the credit scoring process does in fact provide a first line defence against fraud that some of our clients may not be taking advantage of.

If a 'credit decline' application is part of a ruse by a fraudster it's not uncommon for these applicants to manipulate credit vetting data at the point of application to overcome these checks. Changes to address history or to overcome a poor credit background, or income details showing inflated salaries for example, are just two common tactics to try and manipulate a scoring process.

Where a fraud detection process includes velocity rules these amended applications, often resubmitted to test the defences of a company to manipulate credit scores, can quickly be spotted and referred for review.

Obviously, it's essential in order to make use of this functionality that CD data is submitted into your fraud intelligence rules engine and workflow – so that you have visibility of this activity taking place and can factor it into your fraud strategy.

The results of the first tests that the Synectics FCI team ran were impressive. Some 4.2 Million credit declined applications were instrumental in identifying 17,300 records with potential savings of around £33.6 Million in the initial research analysis.

A more recent run of this data then identified 3.7 Million records that were marked as Credit Declines. When assessed against a number of SIRA Finance members national matches the team found 35,698 adverse matches.

Matches derived from these 3.7 Million records were material in assisting in the detection of a further 29,000 adverse applications with potential savings of around £10 Million - and showed potential uplift in fraud identification of around 13%.

Even allowing for processing costs of CD data there was a 10:1 return on investment which is a hefty ROI when trying to reduce losses to shore up the Profit and Loss of any company.

When optimising fraud defences incremental gains can add up to a very significant amount in prevented losses and so it would seem that Credit decline data is one area that client should look at to take advantage of this useful source of intelligence that is already being utilised within the organisation elsewhere.

For more information on the opportunities that this type of data enrichment might offer you please call and speak to your Synectics Relationship Manager in the first instance.

Could a digital ID scheme work and benefit banks and financial organisations?

To find out more about the age of digital identity, join us at our 2019 Conference 26th September

Read more p14

→

With growing calls for a widespread digital ID scheme in the UK, Synectics Solutions Consultant Chris Lewis discusses how such a scheme could potentially work to benefit both financial organisations and consumers.

A digital identity scheme has significant potential to deliver in two key areas; security and simplicity. Both of these are important to consumers and businesses.

> ***"Identify fraud is on the rise and hit an all-time high in 2017, evidenced in data released last year by Cifas. Levels of this type of crime have increased 125% in a decade and it's a problem impacting on consumers of all ages.***

125%
INCREASE
identify fraud

Increasing regulation to better identify and verify customers has been designed partly to tackle the growing threat of ID fraud and although there is a willingness among financial organisations and consumers, current methods are far from the perfect solution.

Consumers find it tiresome having to produce various forms of identification and although they expect their money to be secure, they also expect a seamless customer journey. Digital ID could satisfy both of these requirements.

This scheme could potentially involve two levels of ID profile for each individual – private and public profiles.

Consumers would manage their private profile using a combination of biometric and fact-based verification techniques. This is cross-checked against an individual's "public profile" which is independently created and verified through various 3rd parties – information from credit reference agencies, banks, insurers and employers for example.

Combining these two profile levels would create one unique digital ID for each individual. Consumers access this ID through a secure 'wallet' type application on a smartphone utilising biometric authentication.

The ID could then be instantly presented to a financial organisation, either in person by showing the mobile device or by sharing the profile through a secure transfer mechanism.

Both means of presentation could be backed up with other customer authentication but would be less time consuming and significantly more secure than current methods.

A self-served singular ID of this type would mean that each customer is verified through substantial data and extensive validation which is constantly updated and accurate, making it increasingly difficult for fraudsters to impersonate other people and create false/synthetic identities.

> ***"Technology is crucial to the implementation and practicalities of achieving these benefits but collaboration is equally important."***

Public and private sector organisations need to come together to share data and ensure public IDs are kept 'real-time' and accurate.

It would also ensure that any fraudulent attempts to impersonate and manipulate IDs are quickly determined and analysed, reducing the ability for criminals to try and use an identity across different sectors and for different reasons.

Collaboration will also help to cement national agreement on how to achieve "Digital ID", avoiding the potential for multiple different options that could result in further financial exclusion for certain demographics. A singular methodology will free-up the resources currently invested by companies in multiple levels of customer verification which could be invested in other areas.

Society is not that far from a digital ID scheme. People are already using application processes like 'sign-in with Facebook and Google' and use technology to remember log-in details.

Consumers and suppliers need to be engaged early and be part of the development process, to make a digital ID scheme a reality.

Fraud and Financial Crime in the age of Digital Identity

SYNECTICS SOLUTIONS CONFERENCE

BOOK YOUR PLACE NOW!

synectics-solutions.com/events

Hilton, Tower Bridge London • September 26th 2019

Join Synectics Solutions on the 26th September as we, along with a vast range of speakers, explore the ramifications for fraud and financial crime in a world where a digital identity scheme is widely adopted to authenticate individuals in the UK.

This conference is an important event for those serious about understanding where things stand from the perspective of successfully launching Electronic-ID systems. Key expert speakers from IBM, Equifax, UK Finance, UK Government, The Association Of British Insurers and The University of Portsmouth will all be offering a considered perspective on the current state of progress towards launching digital identity schemes and how this technology is likely to impact fraud and financial crime identification and prevention in the future.

Shaked Vax
IBM Worldwide
Technical Lead for Digital Identity

Rob Kotlarz
Founder,
Digital Identity Net UK

Mark Button
Director, Centre for Counter Fraud Studies,
University of Portsmouth

Rob Malcomson Head of Cross Government Fraud (Data Pilots & Analytics) for the UK Government Cabinet Office • **Matt Burrell** Policy Advisor on E-ID for Association British Insurers • **Jonathan Middleton** Head of Digital Policy Delivery for E-ID • **Peter Taylor** Cybercrime Consultant • **Richard Wood** Synectics Solutions Business Development Director

WHY ATTEND:

- Hear from industry experts
- Network with peers
- Listen to exceptional, high profile keynote speakers
- Learn more from industry bodies
- Choose from a range of targeted breakout sessions

PLUS All conference attendees will receive a free summary report of research conducted specially for the conference by the University of Portsmouth on the true cost of external fraud to financial services companies.

This research assesses and quantifies the wider financial impacts that companies suffer as a result of dealing with the growing issue of fraud and fraud regulatory compliance.

In partnership with

IBM Cabinet Office UK FINANCE ABI EQUIFAX UNIVERSITY OF PORTSMOUTH

#SynecticsDigitalID2019

esure® CELENT MODEL INSURER PRECISION

esure Named Celent Model Insurer for Precision Success

We are delighted to announce that our insurance client, esure, has won a prestigious global award for successfully implementing Precision across its motor insurance division.

The business has landed a Celent 'Model Insurer' award for the significant return on investment it has delivered.

esure's Fraud Investigation Team became aware of a potential gain in the advanced use of motor claim data, to complement current practices in the prevention and detection of fraud.

The company implemented Precision, a pioneering predictive analytics solution from Synectics Solutions which combines sophisticated techniques, machine learning algorithms and expert data science to generate previously unseen insights into its data.

esure's investigation team used Precision to reduce the time taken to detect and identify fraud, and fast-track genuine claim validation to speed up and improve the customer journey.

After deploying the solution, esure saw an immediate 12% increase in crash for cash fraud cases retained for investigation during the first nine months of the project, with one in six claims retained for investigation becoming sourced from Precision.

esure now expects to have delivered a multi-million pound benefit by the end of 2020, with an anticipated net return on investment of 15 to one.

The system has led to a reduction in the time between claim notification and case retention and has helped the productivity and efficiencies of the esure investigation team, allowing them to put the most urgent fraud cases first and reducing the time taken to assign cases requiring investigation by over 50%.

CELENT MODEL INSURER

Celent is a global financial services research and advisory firm for the financial services industry and the annual Model Insurer Awards recognise the best practices of technology usage in different areas critical to success in insurance. esure were winners of the 'Model Insurer' prize in the Data, Analytics and AI category and nominations, submitted by insurance carriers, undergo a rigorous evaluation process by Celent analysts. Celent judge submissions on three core criteria which include demonstrable business benefits of live initiatives, the degree of innovation relative to the industry and the technology or implementation excellence.

Winners of the awards were officially announced at Celent's Innovation and Insight Day at the company's New York offices on Friday 12th April 2019.

After deploying the solution, esure saw an **immediate 12% increase** in the detection of crash for cash fraud

Matt Gilham, Head of Financial Crime at esure, said:

> ***"We are extremely proud of the Celent award which demonstrates the huge strides we have made in our fraud prevention and detection strategies.***
>
> ***"Working with Synectics Solutions, this solution has allowed the team to speed up detection of fraud, as well as improve operational efficiencies."***

Osman Khurshid, Head of Solutions Consultancy at Synectics Solutions, said:

"We are delighted that esure has won this award which shows they are a company at the forefront in terms of fraud detection and prevention.

"It's extremely pleasing to see the significant impact that Precision has had on esure's motor insurance division and the positive return on investment it has had for the company."

Equifax explores how companies are moving toward SaaS and cloud based platforms to make them more agile and change resilient.

By Keith McGill,
Head of ID & Fraud at Equifax

The internet is a game changer. This we have known for some time. What continues to surprise is the pace of change. That is why the digital economy is now king but governments and regulators are struggling to keep up. It's the same for business. Exponential growth in online activity is changing business models. Customer experience is fast becoming the number one focus for any business with a digital proposition. And for those without, extinction looms.

This new paradigm is also driving an alarming increase in fraud. The internet is a fraudster's playground. Synthetic identity, account and identity takeover, organised crime and cyber-attacks have all entered the vernacular and these evolving fraud methods are forcing companies to change how they fight fraud. However, a major challenge to their efforts is how to exploit the overwhelming number of data sources, new technologies and point solutions whilst minimising friction for their digital customer. The reality is that most companies wrestle with how to optimally deploy the fraud tools at their disposal, the result being that fraud losses continue to rise.

To address this organisations are adopting a more holistic approach through deployment of Software as a Service (SaaS) and cloud-based fraud platforms. These give the ability to access multiple fraud services through a single API thereby easing integration demands. Typically, a platform will also include a configurable workflow capability enabling organisations to easily orchestrate the various fraud datasets and tools. IT and operational efficiencies and the ability to orchestrate fraud services are only half the story of course. A fraud platform needs to provide a flexible decision engine that supports rule optimisation. The Holy Grail for all fraud managers is to know which matches to work so that fraud detection is maximised whilst keeping false positives to a minimum. This may sound obvious, after all the ongoing refinement of fraud rules is nothing new. However, where traditionally this would involve looking at fraud matching rules in isolation, advanced analytics is making it easier to investigate and understand the interaction between different data points to create previously unknown predictive segments.

> ***"Significant operational benefits, such as reducing investigation cycle-time, are also achieved now that all referrals can be worked through a single case management system."***

For example, analysis is showing that feeding bureau data directly into the fraud platform, where checks against this data then sit alongside fraud rules matching to syndicated fraud data, can help to reduce false positive rates.

> ***"On a mortgage portfolio for a leading bank, Equifax identified that an income verification check alongside the existing application fraud rules could reduce referral volumes by 85% whilst not reducing the number of frauds identified."***

Income verification check alongside the existing application fraud rules could reduce referrals

85%

Riskier pockets can be similarly identified when overlaying director status or employment validation. This greater discrimination leads to significant reductions in false positives which in turn frees up agents and underwriters to work the high risk cases, helping to improve overall fraud detection rates.

It is not just bureau data that can add value to fraud strategies. Fraud managers are confronted with an ever increasing array of point solutions that come with their own dedicated API: device checks; PEPs and sanctions screening; fraud scores; network visualisation; police intelligence, to name a few. For most organisations it is untenable to entertain integrating these separately; instead to identify a fraud platform that can offer these as micro-services. In this model the platform acts as the application with a collection of services effectively already "plumbed in". This provides fraud practitioners with full access to all the tools required in a single environment from which they can define and amend business rules in real-time.

We should not confine our thinking to fraud. A micro-services architecture enables organisations to use a single platform to meet risk and compliance needs also. Alongside whether a prospective customer looks like a fraud risk, a decision can be made on whether the customer fails regulatory checks or looks a higher credit risk. A fraud platform that means organisations can work compliance and certain risk referrals in the same case management system with all the associated operational efficiencies this delivers.

In summary, fraudsters are exploiting the current technological pace of change better than anyone. To keep up, organisations must develop an approach that successfully leverages the increasing ecosystem of fraud tools and data-sets at their disposal. Fraud platforms provide the most cost-effective way to achieve this and provide the flexibility needed to step in new tools and data-sets as they become available.

Additionally, through sophisticated orchestration and the associated operational benefits, such platforms can ensure that impact to the online customer journey is minimised.

Minimising fraud losses and delighting your online customers. Not always seen as compatible bedfellows. However, developments in SaaS and cloud based models make this much more achievable.

Who are the real victims of misuse of accounts in the UK and where are they based?

Matt Williams, Synectics Solutions FCI Team Consultant, takes a look at who is most affected by misuse of accounts and whether the demographic and geographic evidence is different than we may think.

One of the most interesting fraud trends highlighted within the 2018 data is the increase in the distribution of misuse of account cases, which covers both mules and a variety of payment fraud types.

Misuse accounted for* 36% *of all adverse cases

26% increase on 2017

Now representing **36% of all adverse cases** marked within SIRA, up from just 10% in 2017, it is heavily focussed on Current and Savings Account product lines.

71%

of all marked fraud in Savings was due to misuse

In 2018 the most common threat was ID fraud (80%)

Indeed, within Savings it **accounted for 71% of all fraud marked**, a huge swing from 2017 when Identity fraud was the most common fraud threat (80%).

Whilst the benefits of Current Accounts to an organised fraudster are well documented, and continue to account for the vast majority of fraud cases, Savings Accounts have been traditionally viewed as a low risk product. However, many of these accounts now have similar money transmission facilities to current accounts so are highly attractive to fraudsters, they also tend to come with a lighter apply process due to the lack of credit checking required, meaning they can provide the fraudster with an easier access route into a financial organisation.

For a number of years dealing with the threat of Identity Fraud has been a primary focus for finance clients. To combat this threat, institutions have adopted new technologies, combining traditional data matching with asset profiling and predictive analytics, whilst simultaneously deploying block and deny strategies. These advancements in defences may be having an effect and forcing fraudsters to probe for further ways to both illicit and launder funds, which is potentially via the recruitment of genuine, and perhaps naïve, individuals.

To understand a little more about the misuse fraudster we've taken a sample of data from 2018.
The analysis is based upon sample of 2.5m current account applications from 2018.

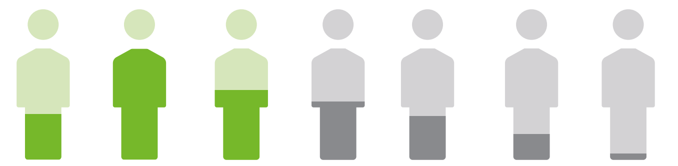
Misuse Rate – Age demographic

0.39% overall misuse rate within the sample

This rate calculated by comparing the volume of misuse cases against the volume of applications received within the sample period.

Age Demographic for Misuse

Diagram showing rates if 1% was the maximum



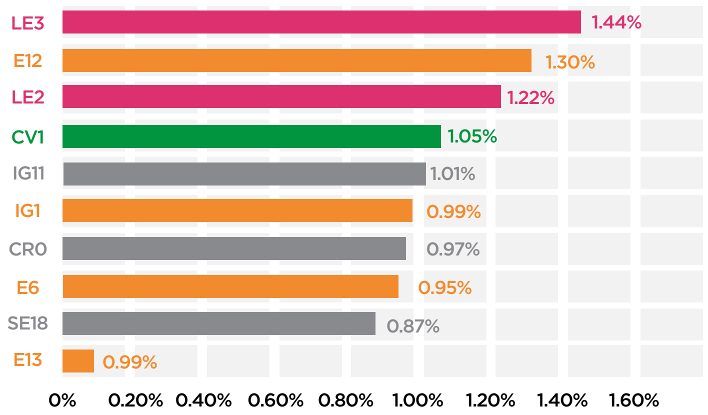
<18	18-21	22-31	32-41	42-51	52-61	61+
FRAUD RATE						
0.30%	0.73%	0.46%	0.39%	0.29%	0.17%	0.04%

68.5% of all misuse cases recorded contain a main applicant under the age of 32.

Although the highest volume of cases appears in the 22-31 demographic, the highest Misuse Rate appears in the 18-21 demographic, the rate being nearly double the average of the overall sample, standing at 0.73%.

Misuse Rate – Location demographic

Top 10 Post Codes for Misuse by Volume

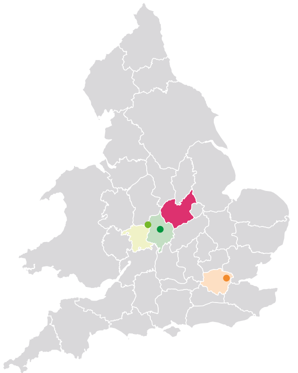


The 10 most prolific areas for misuse of account fraud by volume are listed above.

The areas where volumes are greatest are predominantly centred around London and the Midlands.

As you can see, the misuse rates for these areas are all more than double the average from the sample (0.39%), with the LE3 area of Leicester 3.7 times higher and LE2 some 3 times higher.

Top Grouped Misuse Locations by Volume



If we extend this is to the top 20 by volume and group by City, we can see some definite patterns of activity centred around the Midlands and East London.

Many of the listed post codes are also in close proximity to major centres of higher education or vocational training which may be indicative of targeted student recruitment by organised fraudsters.

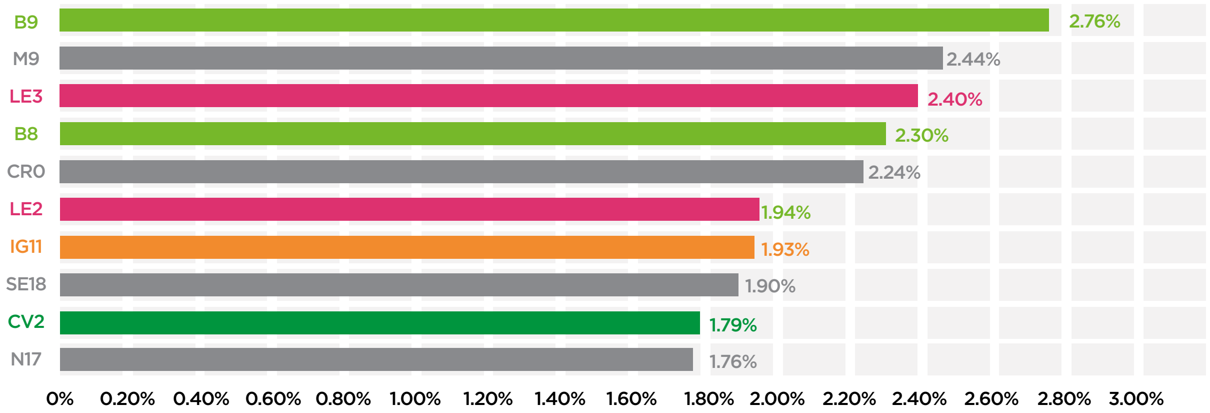
POSTAL SECTOR			
Birmingham B8 B9	Leicester LE2 LE3 LE4 LE5	Coventry CV1 CV2 CV6	East London E6 IG1 E12 IG11 E13 E17
FRAUD RATE			
1.51%	1.27%	0.95%	0.93%

Top Locations for Misuse from 18-21 Age Range

If we now look to combine age with location we start to see even higher rates of misuse.

Within the B9 area of Birmingham, the misuse rate for 18-21 year olds is actually 2.76%, some 7 times the overall Misuse average and 3.8 times the average for the 18-21 misuse demographic.

Even N17 in tenth place has rate some 4.5 times higher than the misuse average and 2.4 times more than the 18-21 demographic.



Conclusion

Identifying misuse intention at application stage has traditionally been troublesome, particularly in a real time decisioning environment, and especially where the data contained within an application is inherently genuine.

Both the statistical data here and anecdotal evidence from our client base points towards organised targeting of the younger population, specifically still in higher education and therefore struggling financially, to facilitate fraud. As is the nature of this fraud type, some of these youngsters will unwittingly get involved without necessarily understanding the full implications of what they are committing to, potentially targeted through many of the social media platforms currently available but equally via simple techniques like word of mouth. However, through greater understanding of the organised fraudsters target demographic and deployment of profiling or predictive models to identify it, we can potentially make inroads into this problem area.

COLLABORATION IS KEY TO TACKLING FRAUDSTERS WHO USE THE DARK WEB AS AN ORGANISED FRAUD PLATFORM

To read more about this fascinating insight into cybercrime fraud, download the full whitepaper at: **www.synectics-solutions.com**

SYNECTICS SOLUTIONS

FRAUD IS NOW THE MOST COMMON CRIME IN THE UK, WITH FRAUDSTERS WORKING TOGETHER TO OPERATE SUCCESSFULLY. COULD COLLABORATION ENABLE ORGANISATIONS TO FIGHT BACK AND GAIN THE UPPER HAND IN THE FIGHT AGAINST FRAUD?

Visit **https://synectics-solutions.com/our-thinking/details/collaboration-enable-organisations-fight-against-fraud**

Research shows that fraud is now the most common crime in the UK with fraudsters working together to operate successfully, often collaborating via restricted user groups or dark web groups to identify weaknesses in target businesses and developing new ways to commit their crimes.

According to the Office of National Statistics there were 5.8million fraud and computer misuse crimes in 2017, making them the most common crimes in the UK. Sophisticated technology is enabling criminals to steal and sell data globally, and to commit fraud in high volumes.

This presents a massive challenge for law enforcement and industries like finance and insurance as we seek to prevent and detect fraud - whilst also providing the high standards of service required to meet ever more demanding customer needs.

The dark web has no search engines and is an unregulated wild-west version of the internet. A place where stolen bank details, weapons, drugs, pornography and just about anything can be bought and sold. Global law enforcement monitors the sites and periodically close them down, make arrests and disrupt the criminals. The downside is that within a few months, new sites spring up and the whole process starts again.

The fraudsters are bold and seemingly fearless. To combat them, we need to understand how they operate across both the dark web and the regular internet.

One of the key findings of this research established that it is very rare for one individual to commit an entire financial crime themselves. Much more likely financial criminals have specialisms (like any place of work) and so will work with trusted partners. One individual will provide data – often from breaches acquired either on the 'dark web' or from criminal networks on the 'bright web'. Another individual will then commit the fraud and then work with another 'specialist ' who will then aid the cashing out process to transfer and launder the money so as to benefit from the crime. The research provides a nice insight into how organised and professional todays financial criminals are.

> ***"People do what they are good at and get others to help with the things they aren't good at. Most can do one or two of stealing data, committing fraud or cashing out, very few can do all three successfully".***
> Brett Johnson, reformed fraud gang leader, 2018.

BUT COULD SECTOR-WIDE COLLABORATION BE THE SOLUTION?

In 2017, Synectics Solutions commenced a project to research organised fraud and cyber crime with the main body of research conducted by Peter Taylor from Peter Taylor Consultants.

Peter's research consisted of meetings and exchanges with cyber security and counter fraud professionals across insurance, banking, online retail and law firms, research on the dark web and restricted sites together with meetings and interviews with selected reformed fraudsters and cyber criminals and an analysis of the fraudsters' training manuals to identify behaviour patterns which are identifiable via technology.

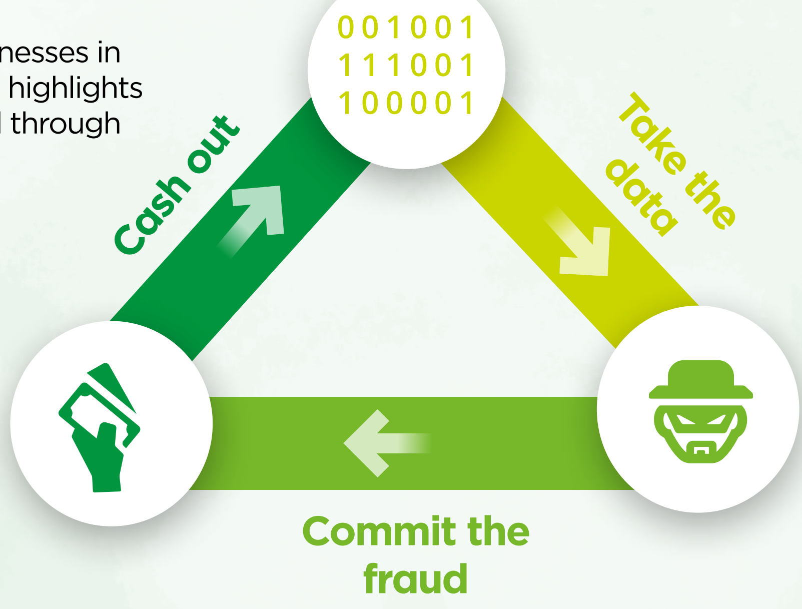
Contrary to popular opinion the most prolific criminals do not steal data, commit fraud and then take the cash. Instead they specialise in crime as a service and the activity they are good at. They are highly dependent on co-operation and collaboration.

In his findings, he focuses on a cybercrime triangle which shows how online fraudsters operate online in the corporate world in similar ways to organised crime gangs.

THE CYBERCRIME TRIANGLE

The Cybercrime Triangle identifies weaknesses in the way fraud is currently dealt with, but highlights opportunities to tackle cybercrime fraud through collaboration and by understanding the 'enemy' and making it harder for them to operate.

Research shows that there is huge improvement in accurate fraud detection where data is kept in a way it can easily be shared, and where analytics are in place.



Latest Fraud Trends – 2018

Our FCI team at Synectics Solutions summarise the 2018 fraud statistics and identify some of the key emerging trends.

HEADLINES

77.1 million submissions made to the National Database in 2018, **up 8.76% on 2017**

54% of motor policy fraud marked at National level (V,F,I) found to be potentially **linked to Ghost Broking**

Organised fraud accounted for 47% of all motor claims adverse in 2018 (V,F,I,S).

Identity Fraud accounted for 44% of all finance records set to Fraud, Inconsistency and Suspect, consistency in 2018 with Misuse of Facility 36%

618K of records set to an adverse status of either Fraud, Inconsistency, Suspect or Victim. **40% of which set to a National Status of Fraud, Inconsistency or Victim and shared with the National SIRA membership**

Current account records accounted for **15% of all finance records**

Total Volume available in National SIRA as of 1st January 2019 **Out of 125 million enquiries 2.7m are adverse**

The average adverse rate across all sectors is 0.80%

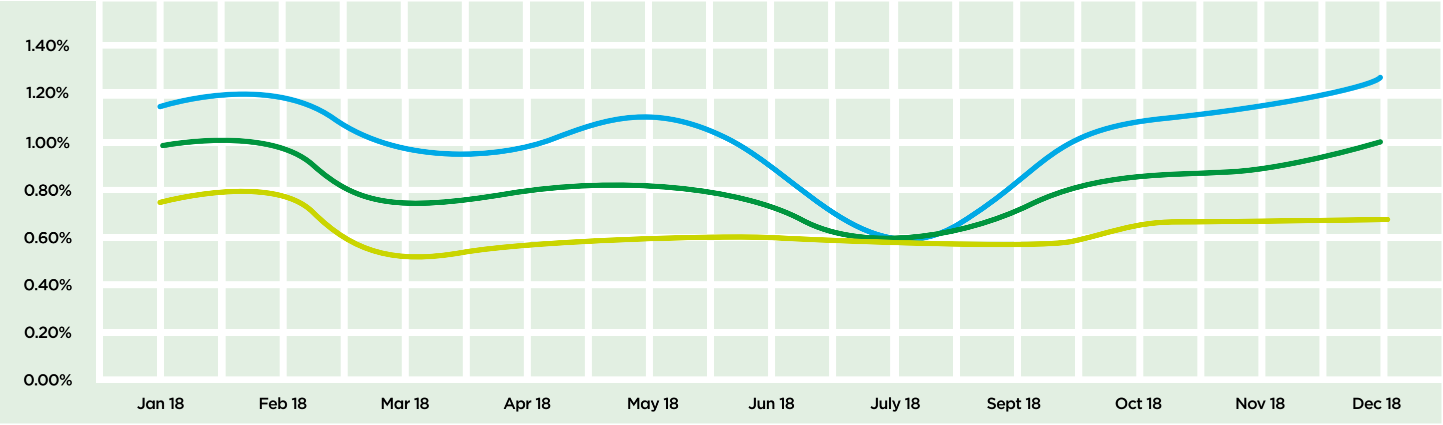
Finance sector being 1% and insurance 0.60%

Total Volume available in National SIRA as of 1st January 2019 **Out of 276 million Parties 5m are set to adverse**

Identity fraud volumes in insurance increased in 2018 with **31.6k of insurance policies set to Fraud, Inconsistency, Suspect or Victim status** with an Identity Fraud related Reason for filing. 18% of insurance policy adverse.

Adverse Rates 2018

The graph below is a summary of adverse rates in 2018.



FRAUD, INCONSISTENCY AND SUSPECT H1 2018	2018 ANNUAL FRAUD RATE
Finance sector	0.99%
Insurance sector	0.62%
Combined	0.80%

Finance Fraud Rate

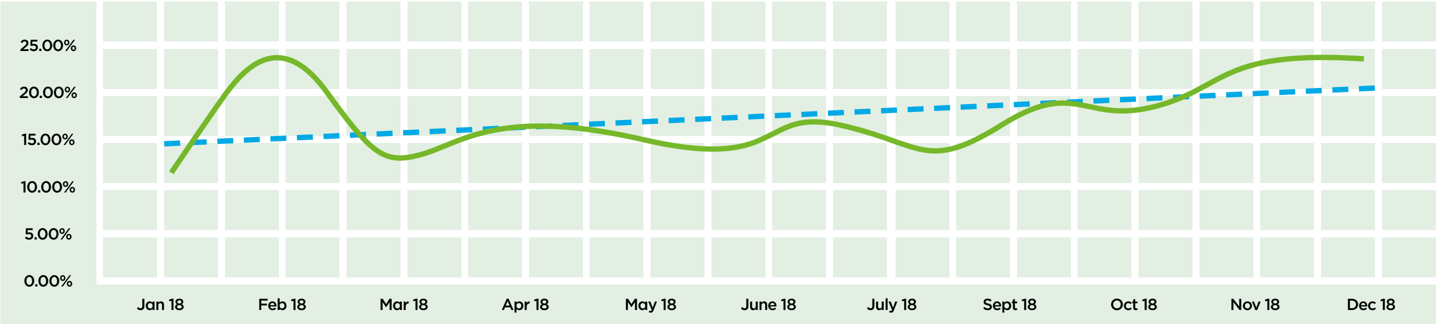
Insurance Fraud Rate

Grand Total

To access the full Fraud Trends Report follow this link:
www.synectics-solutions.com/our-thinking/details/national-sira-annual-fraud-trends-2018

Motor Insurance – Policy Focus

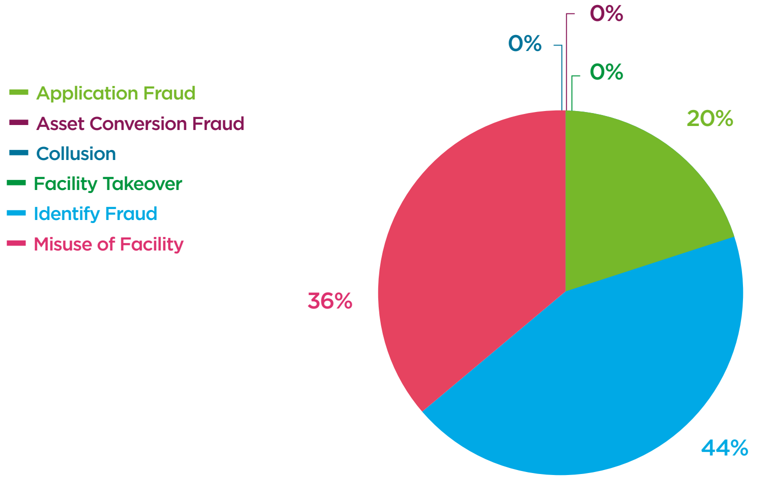
The rise in identity fraud in 2018 has been considerable. Virtually unheard of mid-2016 it now accounts for just under 18% of motor insurance policy fraud at Victim, Fraud, Inconsistency and Suspect level and 40% at National level (Victim, Fraud & Consistency). Starting in January 2018 it accounted for 13% of all adverse and by December it had grown to account for 24% of the adverse.



With insurers enhancing their ID&V checks at Inception stage there is evidence to suggest the fraudster is exploiting the mid-term adjustment process with some insurers. As insurers increase ID&V of the policy holder and named drivers at all stages of the policy and the ever-increasing use of digital channels to service the customer there is the potential for Facility Takeover Fraud to escalate.

Finance – The Aggregated View

Where finance is concerned the volumes of **Identity Fraud related cases actually increased by 10%** but in terms of the types of aggregated fraud type split the percentage share slightly dropped to 44% from 49% in 2017. The percentage share by Application Fraud also dropped from 36% in 2017 to 20% in 2018. The emerging fraud type underlying this change is **Misuse of facility Fraud rising from 15% in 2017 to 36% in 2018**. The shift in the aggregate fraud type split in favour of Misuse of Facility is most notable on products such as Business Banking, Current and Savings accounts.



In 2018 the media pointed attention to APP fraud and accounts being used to receive and launder funds stemming from instances of APP fraud. Along with that questions being asked as to what was being done to educate and protect the public from falling victim to APP fraud and where, if any, does the liability lie to recompense a victim of APP fraud.

It's clear to see from the increase in the percentage split for Misuse of Facility and the volume of records being recorded as Misuse of Facility in 2018 that lateral thinking members are making use of SIRA, Orion and Precision to join the intelligence dots between Application and Post Applications areas. Ensuring intelligence from instances of Post Application, Misuse of Facility, are uploaded into SIRA making full use of SIRA to refer new applications that match to the intelligence. At the same time utilizing Orion to bring to the fore instances of networked cases, invariably of an organized nature.

2019 will be an interesting year with the likes of UK Finance reporting large increases in the instances of APP fraud and monetary losses to victims and what results from the question of liabilities.

2019

SYNECTICS
SOLUTIONS

Synectics Solutions is delighted to announce:

OUR QUEEN'S AWARD FOR ENTERPRISE – INNOVATION 2019

- **Celebrating the success of exciting and innovative businesses**
- **A royal seal of approval for the UK's most outstanding businesses**

This award recognises our innovative products and services and demonstrates our national value.

Synectics is thoroughly proud to have been awarded this highest of accolades for innovation. We would like to thank our talented team at Synectics and our clients who have made a huge contribution to this award.

Managing Director Carol Shanahan said:

"To win an award of this calibre is a fantastic achievement, contributed to by every one of our 360 employees. Of the many awards we have won over the past few years, this is the pinnacle of our work to date.

"Our innovative technologies make a unique contribution to our UK, European and North American customers.

"Our advanced technology and ability to bring organisations together for a common purpose helps identify organised criminal gangs, prevents low level frauds, and makes predictions to block financial crime."

For more information visit **www.synectics-solutions.com**

SYNECTICS
SOLUTIONS

Synectics Solutions Ltd, Synectics House, The Brampton
Newcastle-under-Lyme, Staffordshire, ST5 0QY

+44 (0)333 234 3414
info@synectics-solutions.com
www. synectics-solutions.com