SYNECTICS CONNECT
SPRING 2019 / ISSUE 8

SYNECTICS SOLUTIONS

CONNECT

CONNECTING BUSINESSES THROUGH KNOWLEDGE

UK FINANCE FRAUD ACADEMY

Data breaches in the finance sector

UK FINANCE

SHARED DATA

Is it time for mobile network operators and finance companies to work more closely in the fight against fraud?

FRAUD TRENDS

Why has Push Payment and Mule Fraud become the latest fraud trend to hit our industry – and what can be done to address it?

Data Ecosystems – Is shared data the essential ingredient?

Connect looks at whether intelligence ecosystems, predictive analytics and AI solutions are capable of delivering on their promise

CONTENTS

To find out more about events at Synectics Solutions, please ask your Relationship Manager for an events calendar.

MESSAGE FROM OUR FINANCE DIRECTOR, ROB MOORHOUSE

I was appointed Finance Director here at Synectics Solutions back in 2013. Prior to that I had already spent 20 years with the company, involved in business development, relationship management and systems delivery.

Our number one priority in the finance team is to ensure that we always have the money available to meet our commitments and fund all of the good things we plan to do. This involves working with customers, staff and suppliers to ensure that our commercial management systems work in everyone's best interests and the cash continues to flow.

As with any finance team, we also have a host of other responsibilities that keep us busy; maintaining accurate records, complying with tax regulations, handling payroll queries, building good relations with our bankers and producing our annual accounts.

Above and beyond the day job we also strive to be a key player in the future change and growth of the business. Financial analysis and reporting provide a common platform for all areas of the business to review the impact of their management decisions.

The financial numbers are not the only measure of success, by any means, but they do provide an easily accessible set of tools for collaborative decision making. We are also involved in the preparation of individual product plans and business cases to help assess the particular risks and opportunities associated with new initiatives and ongoing investment decisions.

Activities across every aspect of a business have an impact on the company's financial performance and we aim to provide an insight into the financial health of the company through a series of projections covering the 5-year business strategy, annual business plan, and quarterly tracking reports.

I firmly believe that finance is a key component of the general management team and plays a critical role in the overall success of the business.

SIRA

Welcome to the very latest SIRA members!

As the National SIRA database continues to grow you will benefit from being able to access and interrogate intelligence from a number of different industries and types of organisations.

The database is continually updated and enriched giving you greater access to accurate, timely and relevant data to enhance your investigations and build a strong foundation to configure your detection and prevention rules and models upon.

Welcome to our new members! Current members should consider these new data feeds when assessing referral rates.

MS&AD Aioi Nissay Dowa Insurance

As part of the MS&AD Insurance Group, Aioi Nissay Dowa Insurance Group (ANDIE) is a major insurer that operates in two distinct markets. Firstly as a white label insurer, acting on behalf of its partners and secondly as a direct business insurer. ANDIE will be utilising SIRA and our Real-Time Quote service from early 2019.

Hedgehog

Founded in 2017, Hedgehog Insurance offer motor policies for UK consumers. In November 2018 the company went live with SIRA and our Real-Time Quote service.

Keystone Property Finance

Keystone Property Finance is an intermediary-only lender, established to aid brokers in sourcing specialist buy-to-let finance. Keystone went live with SIRA in October 2018.

PSA Finance (Via Equifax UK)

Offering car finance and insurance products, PSA offers consumer motor finance agreements for customers looking to purchase a Peugeot, Citroen or DS vehicle. PSA use SIRA to screen all motor finance applications in real-time.

RSA

RSA is one of the world's longest standing general insurers servicing individuals and small and large businesses. RSA has chosen our SIRA Real-Time solution with the additions of SQL and Device Profiling (provided by iovation through SIRA).

HABITO (Via Equifax UK)

Habito is an online-only mortgage broker that searches and offers the best mortgages for their customers. Habito use SIRA to check new mortgage applications in real-time.

White Oak UK

Formerly LDF, White Oak UK is a well-established lender that provides entrepreneurs and business owners with finance to support growth. White Oak UK is using SIRA and has integrated additional data from National Hunter within its solution.

freeway insurance services

Freeway (via Equifax UK)

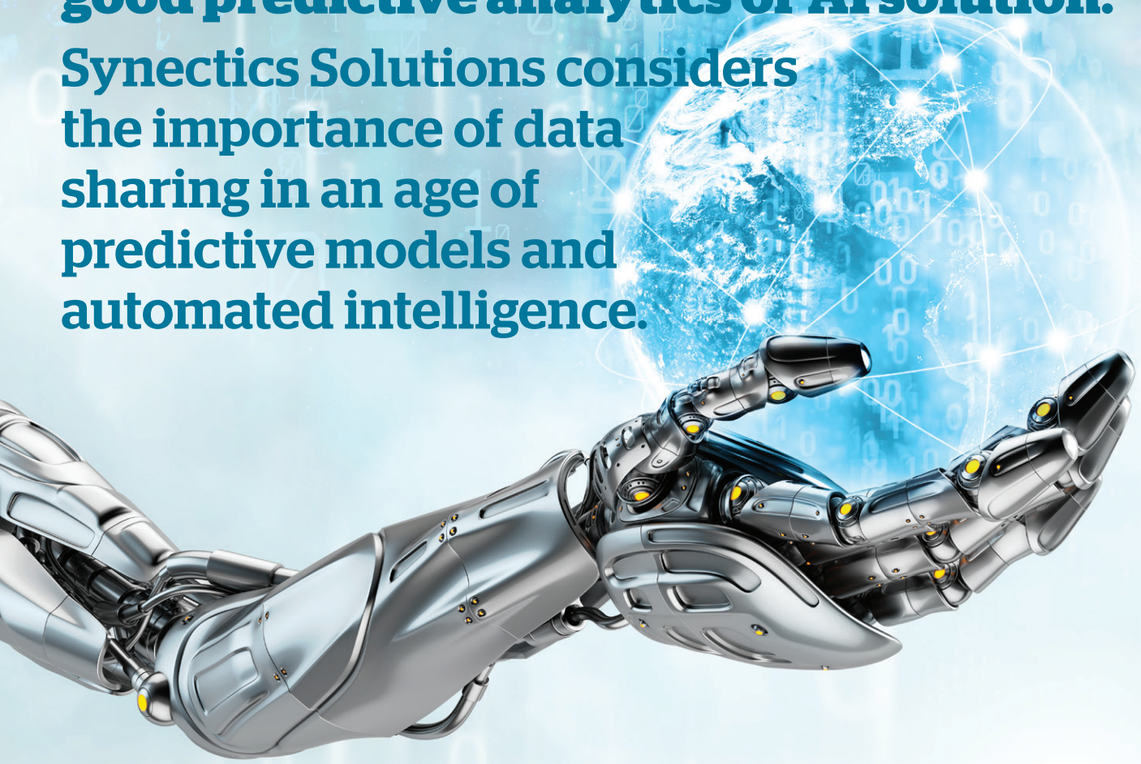
Freeway is a motor insurer specialising in cover for taxi drivers. Freeway screen policies and quotes in real-time via SIRA.

BrokerDirect Plc
A better way to insure

Broker Direct is a general insurance management operation for brokers, which went live with SIRA and our Real-Time Quote solution in October 2018. Broker Direct use SIRA to screen motor policies and claims.

Data Ecosystems – Accurate, timely and highly correlated data is the lifeblood of any good predictive analytics or AI solution.

Synectics Solutions considers the importance of data sharing in an age of predictive models and automated intelligence.



Much has been written recently about how artificial intelligence, machine learning and predictive analysis are going to reshape the world we live in. Automation, robotics and the impact that these technologies will have on our jobs and daily lives is forecast to bring some of the most systemic changes to our existence.

Certainly, in the area of fraud and financial crime prevention, there has been tremendous excitement about how innovative technology and intelligent data eco-systems will enhance the way we identify, address and prevent financial crime. Synectics Solutions have been very much at the forefront of this debate as we are the custodians of one of the UK's leading fraud prevention and detection intelligence resources – National SIRA. The shared database is one of the shining examples of how consortium data has become tremendously successful.

Synectics have also invested considerable capital in bringing leading edge predictive techniques to the market to enable our clients to integrate predictive analytics into their data ecosystem and enhance their ability to stay ahead of financial crime and fraud.

CAUTIONS FOR EMBRACING NEW TECHNOLOGY

However, **it's incredibly important to not get lost in the hype** when new technology is ushered in and heralded as the new shiny tool. One of the topics that's being very much debated currently is the place for consortium data in a world of machine learning and predictive analysis. Ultimately, there is no substitute for accurate, relevant and timely data to feed the models and algorithms that all of these automation and data science tools use to produce their insight.

It's a hard fact that when it comes to predictive analysis, the information source that will be most valuable in the fight against fraud is proven fraud data – and lots of it. Of course there is a myriad of other data sources that can help to inform decisions around fraud. But the law of statistics doesn't change when it comes to predictive analysis. The more data you have, the better your models will be. And if that data is highly correlated to the very thing you are trying to predict then you are on to winner!

"Staying competitive in the future will come down to what data you have and how you filter out the noise. From there, success will be determined by how well you're using the information to drive value in the market."

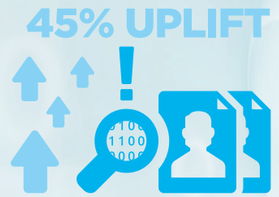
Scott Penberthy, Director of Applied Artificial Intelligence, Google Inc.

HIGHLY CORRELATED DATA IS ESSENTIAL FOR PREDICTIVE ANALYSIS

Certainly there are some who might try and mitigate the risks by leveraging their own data as best they can. But at the end of the day, the cold truth is, what's going to work better; 10,000 data points, loosely correlated to your target or 200 million data points that have a very high degree of correlation?

In fact, Synectics recently performed a pilot study for one of our major banking clients to look at this very topic. We took a sample of the clients own data and ran a number of statistical models in Precision, to help predict a variety of fraud behaviours. We then ran those same models and included intelligence from the National SIRA database.

The models that had the use of consortium data (in addition to the clients data) were seeing a 45% uplift in the amount of fraudulent applications being detected.



You don't even have to be a statistician to know that's a pretty hefty uplift, and one that would have considerable ramifications for accuracy and credibility in a live business environment.

MAXIMISING DATA TO SECURE YOUR BUSINESS

That's not to say that there is no use for in-house data, or calling out to other data sources to enrich intelligence. This will certainly enable a richer variety of nuanced decision making to help align fraud strategy to a commercial strategy. At Synectics Solutions, we have partnerships with many third party organisations, which allows us to offer a number of additional data sources to our clients. These data sources include; Cifas, Dow Jones, Crif, CUE, Ministry of Justice, The National Fraud Initiative and the Insurance Fraud Bureau.

Ultimately, the truth is that in this world it's not an either/or equation when it comes to deploying some of these technologies. Maximising the amount of relevant, accurate data, and enriching that data with your own or third-party sources, is what's going to deliver you the kind of financial crime solution that will secure your business, and protect your customers in the future. All too often one hears about companies building data models and then forgetting that the world moves on.

"Unless the data sets that the models are drawn from are constantly reflecting what is happening today, those companies are effectively predicting the past and not the future."

Consortium data is an excellent resource in this respect as it is kept relevant by the nature of the community keeping it up to date.

We're delighted that we are now seeing a wider range of business sectors feeding data into National SIRA that includes everything from the full range of banking products, various insurance lines (from motor, home, commercial and recently pet data) as well as car rental, asset and motor finance data. We're all aware that the criminals continue to infiltrate across a number of sectors and product lines. This commitment to sharing cross-sector data from our members is only making it more difficult for the fraudsters to operate across sectors.

The upshot is that we believe that by working closely with our clients and helping to input into their data strategy, we can leverage the National SIRA consortium intelligence and continue to drive improvements to reduce the impact that financial crime has on our clients.

The National Fraud Initiative

The National Fraud Initiative (NFI) is part of the UK Government's fraud prevention strategy, which has prevented over £1.69 billion of payments made fraudulently or in error. The NFI exercise is undertaken by Synectics Solutions on behalf of the Cabinet Office.

Through this exclusive partnership the data collected through the NFI is now available for private sector organisations to match to in SIRA.

The 20+ new data sets include state and housing benefit information, council tax data, deceased person records and social housing waiting lists.

Pet Insurance

We have a number of clients who use SIRA to screen their pet insurance claims and policies.

Pet insurance is one of the fastest growing lines in the UK with £706 million paid out in claims in 2016 alone. This increase will inevitably be attractive to the fraudsters.

By matching to pet insurance adverse members of the SIRA syndicate are able to identify and block yet another potential entry point for the criminals.

Motor Finance

Over the last few months we have started to work with two leading motor finance providers that are now contributing to the National SIRA syndicate.

These providers join a number of existing clients who already add adverse motor finance applications to National SIRA.

As the motor finance sector continues to grow, driven by the increasing popularity of Personal Contract Purchase, the risk of financial crime becomes ever-greater. It is becoming evident that motor finance providers need to check and validate potential customers more closely than ever before, whilst at the same time delivering the swift and seamless service which the market demands.

QBE – EUROPE'S LARGEST BUSINESS INSURER BENEFITS FROM AWARD-WINNING DATA SHARING SOLUTION TO ENHANCE FRAUD PREVENTION STRATEGIES

Insurance Times | **AWARD WINNING TECHNOLOGY**

EXCELLENCE IN TECHNOLOGY

QBE, The Cabinet Office and Synectics Solutions.

SITUATION

In recent years, leading business insurer QBE has sought to increase and enhance its automated fraud detection capacity using new methods and data sources. QBE wanted to identify additional sources of intelligence to help them spot more fraud across insurance applications.

The fraud team also wanted to see an uplift in the amount of fraud detected for previously investigated cases, by retrospectively matching to records, previously marked as fraud. In particular, they wanted to look at exaggerated and fabricated, third party motor and casualty claims, to see if there was any correlation between fraudulent benefit and insurance claims.

SOLUTION

The Cabinet Office is responsible for the National Fraud Initiative (NFI). The aim of the NFI is to protect public services from fraud and error, saving tax payer's money through sophisticated data matching and analytics. In 2017, the Cabinet Office and Synectics Solutions began a proof of concept to evaluate the potential to utilise NFI data to assist the insurance sector with detecting fraudulent claims.

"The NFI has already enabled participants to prevent and detect fraud in excess of £1.69 billion and we are always seeking to help target new fraud risk areas. We are delighted to now be working with Synectics and QBE to use the NFI to assist the insurance sector in its fight against fraud. The initial results are really impressive and demonstrate huge potential."

Darren Shillington, Head of the NFI Team, Cabinet Office.

This was the first time that public sector data would be available to private sector organisations for fraud prevention purposes. QBE's requirements for the integration of public sector data within their SIRA system offered the perfect opportunity to trial this new collaborative, cross-sector data sharing initiative.

RESULTS

QBE has now integrated the service into a live environment and so far the data is showing a significant positive impact. Consequently, **the public sector data is now available to the insurance and finance sectors,** through National SIRA, to improve fraud prevention capabilities. The NFI intelligence includes: housing benefit claim data, social housing waiting lists and more.

45% 45% uplift in the identification of potential fraudulent claims for QBE, by integrating NFI data into SIRA.

QBE has seen a significant impact on how claims would have been handled had the insurer had access to the public sector data at the time of the claim.

41% In a live environment, for the first quarter, QBE set 41% of applications to fraud, suspect or under investigation.

"Insurance fraud remains a major issue in our industry, but through collaboration and sharing of data, we are able to better detect and combat fraudulent claims. Working with Synectics and the Cabinet Office has already had a positive impact on our fraud identification and claims handling and we look forward to working together to fight these types of crimes."

Jon Radford, Special Investigation Unit Claims Manager – QBE European Operations.

For more information about how you can integrate the NFI data sets within your SIRA system please contact your Business Development Manager on 0333 234 3414.

SIRA Real-Time

ROBUST FRAUD CHECKS v CUSTOMER SATISFACTION

With increasing pressure on organisations to fully understand who they are selling products to, plus the demand from customers for instant access to financial and insurance products, service providers have a fine balancing act to undertake to esure they are underwriting business competitively, and with reduced risk.

INTRODUCING SIRA REAL-TIME

SIRA Real-Time from Synectics Solutions gives you access to the very latest information on potential high risk applications , to enable you to male truly informed decisions at all stages of the customer application process.

The dynamic nature of SIRA Real-Time means you can create bespoke verification, risk and compliance checks using your own local data, but also match to data held in the UK largest database of known fraud cases, in addition to a number of leading multi-sector third-party data sources through Synectics' agnostic data marketplace.

SIRA Real-Time gives you the flexibility to screen customers against those submissions that were previously considered as genuine or clear and increase efficiencies so your team can identify and address the most serious cases of financial crime first.

This new functionality will help you to be more agile and identify emerging patterns in applications, as well as detect the manipulation of applications throughout the customer boarding journey.

Compared to traditional batch data matching systems, SIRA Real-Time will help you to board customers in a matter of seconds rather than hours or even days. What's more all decisions and outcomes are updated, with the ability to orchestrate and update the customer application lifestyle in additional systems, which removes the requirement for manual intervention. This helps smooth the customer journey and remove the risk of manual error.

Ultimately, SIRA Real-Time gives you the comfort that you are providing services to genuine customers, in a time frame that satisfies them and you, with reduced risk.

"Businesses need to implement financial crime prevention systems that provide actionable insight, to help them immediately assess the risk associated with an application, without disrupting the customer journey."

There's no compromise on the number of rules, allowing you to receive actionable insight in real time immediately.

Prompt results which enable you to make decisions immediately to increase the efficiency of your customer boarding processes.

Multiple rule sets allow rule flexibility, including velocity and clear matching, enabling a wider use of matches regardless of status.

Confidence that you are completing all the necessary customer identification and verification checks to satisfy regulatory compliance such as Know Your Customer, Anti-Money Laundering obligations.

Commercial advantage to ensure you remain competitive in a growing and fast paced market.

Increased efficiencies so your team can reduce their workload and prioritise the most serious cases of financial crime first and bring them to the forefront of the customer journey.

Satisfy your customers and regulatory commitments in a fast paced and competitive market with SIRA Real-Time – the ultimate solution to enhance your financial crime and fraud prevention strategy.

Call your Business Development Manager on: 0333 234 3418 or visit www.synectics-solutions.com

THE GROWING THREAT OF MULE RECRUITMENT AND AUTHORISED PUSH PAYMENT FRAUD

To read more about APP and Money Mule fraud, download our latest whitepapers at **www.synectics-solutions.com**

Visit **https://www.synectics-solutions.com/our-thinking/details/authorised-push-payment-fraud** to find out more about addressing the growing problem of Authorised Push Payment (APP).

Visit **https://www.synectics-solutions.com/our-thinking/details/money-mule-fraud** to find out how we might respond to more and more young people becoming involved in Money Mule Fraud.

As fraudsters continue to focus on exploiting vulnerable people and small businesses to commit a wide range of Authorised Push Payment (APP) 'scams' and target people as money mules what can you do to address the problem?

In response to the Which? super-complaint of 2016, the focus has moved to the responsibilities of financial institutions – with UK Finance and the Payment Services Regulator consulting with members to establish best practice. In all such situations, prevention is better than cure. So, is there a way that financial institutions can fight back against the growing problem of APP fraud and money mules?

What is APP Fraud and who is affected?

Authorised Push Payment (APP) fraud occurs when a financial criminal dupes an innocent party into sending a payment under false pretences to a recipient bank account the criminal has control of.

This type of fraud can happen to both private individuals and businesses and, as payments are typically made in real-time, funds can be quickly moved on or directly withdrawn without revocation, and before an innocent party even realises they have fallen victim to a scam.

Money mules – another growing problem

Another challenge financial organisations face is the insatiable demand criminals have for money mules to help them launder the proceeds of crime.

Genuine people can be recruited knowingly or unknowingly to act as money mules or have their accounts or identities compromised to facilitate money laundering activity.

Young or old, knowingly or unknowingly involved, mules are targeted because they are vulnerable. Students are attracted by the promise of quick cash and for older people their trust is easily exploited by fraudsters.

Since 2013, the number of young people identified as having money mule accounts has more than doubled – there was a rise of 26% last year alone.

Addressing the problem

At the moment, there is no 'silver bullet' solution to preventing APP scams or money mules. The regulators have cited collaboration and data sharing as key factors in mitigating the risk of APP fraud. Many bodies, from financial crime solution companies like Synectics Solutions to banks and trade groups, are working together to try to formulate better systems to combat the problem, including transactional controls and flagging up potential and actual victims – whilst providing efficient real-time 'on boarding' service to genuine customers.

Achieving this will take a holistic approach, looking at both the application process and account lifecycle and offering a multi-layered set of provisions and solutions.

Synectics Solutions is well equipped to support the industry in meeting these challenges, hosting an established syndicated intelligence database of records across multiple sectors and with access to a variety of other public and private data sources. In harnessing this data **our established SIRA and Precision services have a key role to play in the future of the fight against APP scams and money mules.**

SIRA is an all-in-one established financial crime prevention solution which leverages millions of data items from different sectors to identify and stop fraudsters working across industries, enabling providers to make quick and informed decisions. It works using a multitude of machine learning algorithms and comprehensive workflow management enabling point of application identification of fraud cases, whether these be identity frauds or money mules.

Precision, our predictive analytics solution, has the ability to process huge volumes of data and apply a combined array of algorithms and modelling techniques. It provides a predictive modelling platform capable of analysing the largest of data sets and producing actionable results in real-time. Increasingly it is being used to target specific types of financial crime activity.

This may prove to be particularly helpful in:

- **Profiling what a potential victim of APP scamming might look like, taking in factors like demographics, age, income, location and occupation**
- **Identifying bank accounts applied for by first party and third party fraudsters where the account if opened has a high risk of being used for mule activity, namely being used to receive funds as a result of fraudulent activity elsewhere, account takeover or APP**

However, we appreciate this is only part of the solution. We are also taking an active role in this initiative, collaborating with customers and the industry to move the fight against APP fraud and money mules forward.

We are co-ordinating shared knowledge through workshops and feedback from our clients – financial institutions which are on the 'front line'. We're also tracking the voluntary Contingent Reimbursement Model Code currently being applied by many banks to compensate victims of APP fraud – and we will consult with our members when this code is ratified.

Whilst there is a lot of industry focus in this area there is also some uncertainty on how best to combat it and the full implications of the PSR guidelines. What is certain is that financial institutions which fail to take up a positive and proactive position are leaving themselves open to potential damage, financially and reputationally.

To discuss the implications of APP fraud and money mules and how you might participate in the collaborative approach to combating the problems, please call 03332343418, email info@synectics-solutions.com or visit www.synectics-solutions.com

UK Finance Economic Crime Academy

UK FINANCE

Webinar #1:
ADDRESSING THE GROWING THREAT OF IMPERSONATION FRAUD IN FINANCIAL SERVICES

During the webinar it was evident that identification fraud was still a growing, and by far the biggest concern, amongst the audience of 336 finance professionals – with 42% of them highlighting this as the area where they have seen the biggest growth in fraud over the last year.

This pattern was reflected in the trends analysis from our Financial Crime experts, looking at data from the National SIRA database, where 50% of classified fraud, on financial products, was due to identification fraud.

More interestingly, webinar participants emphasised a marked concern over misuse of facility, which is a type of fraud where an innocent victims' genuine information or account is used to apply for credit or transfer funds to and from illicit accounts.

FREE WEBINARS IN 2019

Webinar #2 looked at **the importance of collaborative data and predictive analytics in the fight against fraud** which aired at the end of January.

We are hosting 2 more free webinars in April / May and September 2019

Watch this space for more details

Prior to the webinars we will send you a link with more information on how to book your place.

UK FINANCE

The rising influence of data breaches in financial fraud

Ross Webster, Head of Fraud Intelligence at UK Finance

Data breaches and their impact on financial fraud are not new. However, at UK Finance (through our intelligence team) we have a unique view on how these events influence the threat landscape in a variety of ways – from online fraud to the rising threat of SMiShing.

When you think of recent high-profile data breaches you immediately think about the risk they pose to the affected customers' accounts e.g. card information which can be used to carry out unauthorised transactions. However, this can mean the full impact of the breach, along with the risk to victims and the public, is not always fully understood.

Whilst it is right to first look at the accounts that are immediately vulnerable, we should not lose sight of the fact that often a much greater data set relating to customers may have been compromised. This can put customers at risk of a variety of fraud attacks.

"A data compromise of even minimal data sets, such as email addresses, can be the precursor to identity theft, account takeovers, or even authorised push payment fraud."

Victims are increasingly targeted by criminals who use 'social engineering' tactics to make the attack more successful, by persuading customers to hand over personal information which can further enhance data sets or by duping customers into transacting on their behalf.

Over the last couple of years the threat associated with SMiShing has continued to grow, with this form of fraud now seen as a key data harvesting tool for criminals.

Personal data continues to be an extremely valuable commodity to the criminal fraternity and almost an industry in its own right. This has resulted in the compromise of data and its subsequent use not always being linked. Data is sold, re-sold and enhanced regularly by vendors collecting it from multiple sources. This makes fraud attribution and proactive victim identification a challenge.

In addition to direct attacks on customers impacted by breaches, criminals continue to use these high-profile events as triggers to target unaffected customers. Referencing these incidents in subsequent phishing and SMiShing campaigns provides criminals with a believable rationale for a first point of contact.

By playing on scare tactics and the reach of household brands, criminals believe they will achieve higher success rates. This type of attack may also become more prominent following the introduction of GDPR, which means firms must now disclose data breaches, giving criminals the opportunity to 'piggyback' on such events.

"There is no silver bullet to stop the increasing influence of data compromise on financial fraud. However, this is not solely a financial sector problem, data breaches are likely to be a risk factor in many industries."

Collaboration remains a key weapon in the fight, with good communication and the sharing of intelligence needed to ensure mitigation is effective and efficient.

Alongside this, promoting good customer behaviour through the Take Five campaign is essential, encouraging the public to protect their personal data, and educating them on the risks of failing to do so. For more information visit **https://takefive-stopfraud.org.uk/**

PROTECTING CONSUMERS AGAINST identity THEFT – WHOSE RESPONSIBILITY IS IT?

In September 2018 it was widely reported that 50 million Facebook users had their accounts breached, and by its own accounts, Facebook estimate that as many as 270 million of its user accounts are fake.

Social media providers are under increasing pressure to tighten controls on advertising and privacy and become more transparent and consistent when it comes to educating users on how to protect themselves and their identity.

A RISE IN IDENTITY THEFT

As consumers develop a more relaxed approach to using social media and sharing information online, they are leaving themselves highly exposed to becoming a victim of identification theft, account hijacking or impersonation and identity fraud. And it's not just the younger generation leaving themselves at risk. Recent data[1] from the National SIRA database shows that the 40+ generation from affluent areas, of stable credit background, and middle to high incomes continue to be the main targets of identity fraud. For the fraudsters, with fairly low resource and investment, they are able to glean innocent victims' details, from social networking sites, through a series of calculated scams, which once harvested can help the criminals perpetrate more serious cases of fraud and financial crime.

"As the opportunities for fraudsters to gather identification details online increase, inevitably so do cases of identity fraud."

The genuine person's personal details are a dream for the criminals – having access to this information opens opportunities to apply for financial products and services using genuine, clean details that wouldn't necessarily be denied at applications stage. In a recent report[1] Synectics Solutions reported that cases of identification fraud accounted for 50% of cases of fraud recorded in the National SIRA database. The question to ask is, whose responsibility is it to protect users of social media against identification fraud and reduce the number of cases we are seeing? Is it the consumers themselves, the social networking providers or the financial services providers?

1: www.synectics-solutions.com/our-thinking/details/connect-edition-7

HOW SYNECTICS SOLUTIONS IS HELPING CLIENTS

At Synectics Solutions we have been working closely with our clients to develop a 'Victim' status in SIRA. This allows clients to share information, with other members of the SIRA syndicate, when an innocent victim's identification details have been stolen or compromised, then used to apply for products and services. This new development is helping to protect those that have been targeted by the criminals by ensuring they won't be adversely affected in the future.

We spoke to one of our clients and a financial crime expert to find out their thoughts and what work they are doing to protect consumers against identification theft...

"I strongly believe we all have a part to play in tackling this concern and I can see instances of that beginning to take place. The social media industry needs to continue to educate their users regarding security settings and the risks of providing certain pieces of personal data in their profile. Financial service providers need to continue to educate their audience on the risk of sharing personal information online and work collaboratively with fraud prevention agencies in response to instances of major data breaches."

"Persons that are victims of a data breach are inherently more at risk of being victims of impersonation or account takeover. Having pointed a finger I have to finally say that you and I need to give thought to the personal information we share and take simple steps to ensure we have the correct security settings in our profiles blocking out undesirables from accessing our profiles."

Kevin Carradine, Financial Crime Expert, Synectics Solutions

Santander

Research carried out by Santander among 18-24 year olds revealed that 85 per cent have shared details on social media that could help build a personal profile exploitable by fraudsters. A Santander spokesperson said:

"It's extremely important that people are cautious about the information they share online so they don't become a victim of identity theft. Our advice to customers to help protect themselves includes: shredding sensitive information such as bank account statements, deleting suspicious emails, especially any asking for personal details, and generally thinking twice about any information which they share online. People can also take measures such as redirecting their mail if they move house and use online bank statements instead of printed, postal ones."

Creating a multi-layered fraud prevention strategy aligned to your business goals requires more than just software

Synectics provides a range of expert advice and insight to ensure that you gain true value from your SIRA fraud platform – as well as helping your fraud and data strategy teams to avoid some major pitfalls when boarding new customers

Fraud and financial crime is continually changing. As soon as you control it in one area of your business, the criminals will have perpetrated another area, and will be working to exploit the next. And the likelihood is that your competitors are experiencing the same challenges as you.

So – will you choose to fight it alone with the risk of continually chasing the criminal, or work together with like-minded experts and professionals, who are driven to stop illicit activity at the earliest opportunity?

FRAUD AND FINANCIAL CRIME CONSULTANCY SERVICES

At Synectics Solutions we have been pioneering collaborative data services and financial crime prevention solutions for over 25 years. During this time we've built up an enviable body of expertise, helping our clients to detect and prevent nearly £6 billion of fraud across both the private and public sectors.

As part of this journey we have acquired a highly skilled, multi-disciplinary team including fraud and financial crime prevention experts, data scientists, systems architects, process engineers and a team of skilled software developers.

Our experts have decades of experience and are passionate about helping to stop fraud and financial crime in all its guises.

They keep abreast of the latest regulations as well as having constant dialogue with our client base and the industries we operate in, to understand the latest threats and challenges and help them optimise their financial crime strategy.

"Our experts have decades of experience and are passionate about helping to stop fraud and financial crime in all its guises."

OUR SERVICES

Financial crime resource and strategy assessments

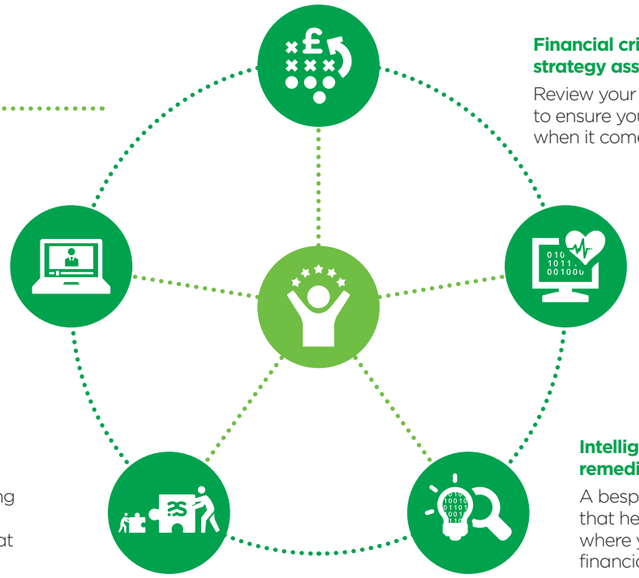
Review your customer acquisition strategy to ensure you are adopting best practice when it comes to fraud prevention.

Systems training

Software training sessions to make sure you and your teams are making the best use of the technology we deploy on your behalf.

Data health checks

Manage your data in the most effective way possible, to unlock its true value.



Solution optimisation

Have the confidence that your teams are adequately leveraging and utilising the systems and intelligence to effectively combat financial crime.

Intelligence analysis and remediation services

A bespoke data analysis project that helps you quickly identify where you may be exposed to financial crime or fraud.

GET IN TOUCH

Our consultancy services can give you peace of mind that your organisation is adopting the latest technology and strategic best practice to defend against an increasingly complex set of threats and an ever escalating burden of regulatory requirements.

You'll never stop fraud and financial crime on your own. Call your Business Development Manager on 0333 234 3414 to find out how you can work with our experts to optimise your fraud prevention tactics.

PRECISION

Forecasting and controlling the cost of insurance claims

The ABI have recently reported a marked increase in the volume of insurance claims across different product lines. The news for consumers is good with insurers paying over 98% of claims with an average of £23 million a day paid out by motor insurers. However, the news for underwriters is not so good if the claims and settlement forecasting thresholds have been seriously underestimated – costing the business more in the long run. Connect looks at the early identification of 'jumper claims' which have a high potential to become costly.

Motor insurance is not the only line of business that has seen a growth in the number of claims made. A rise in the number of consumers purchasing expensive gadgets has caused a significant uplift in Household Contents claims either as a result of thefts from the home or under 'Items Away From the Home' policy extensions. A number of flash floods in the UK during 2018 have inevitably caused a surge in both Buildings and Contents insurance affecting both domestic and commercial properties, even pet and travel insurance have not been immune to these rises.

The insurance industry continues to experience year-on-year increases in claims acceptance rates where private motor claims rose by £50, with 98% of claims paid out and the average domestic property claim increasing to £3,400.

Figures are from the Association of British Insurers, State of Market, 2018 (www.abi.org.uk/globalassets/files/publications/public/data/abi_bro4467_state_of_market_v10.pdf)

"As the number and cost of claims continue to rise, insurance companies are coming under increasing pressure to forecast and control the impact that these increases will have on revenue, to help them remain competitive in a growing market."

Utilising predictive analytics for claims

Synectics is working with a major UK insurer to enable the early identification of claims that have a low cost, early in their life cycle, but have a high potential to become costly – also known as jumper claims. The way a company manages the claims process and in particular the reserves associated with those claims is fundamental to its profits and long-term sustainability.

In an increasingly complex market, insurance claims teams can no longer rely on individual experience and judgement alone to manage reserving.

Tools like predictive analytics that augment and accelerate decision making and processes are fast becoming a necessity for insurers.

Identifying jumper claims

Experienced claims handlers and loss adjusters can identify many of the early warning signs that indicate certain claims could escalate into larger losses for an insurers. However, due to the volume of data being analysed and the possible variables, some potentially severe cost escalations can be missed resulting in significant and potentially unaccounted for financial exposure.

"By integrating predictive analytics through Precision, our client has been able to analyse their current claims data, using advanced statistical models and bespoke algorithms, to understand and monitor the patterns and trends that constitute a jumper claim."

This translates in to accurate forecasting and being able to predict the likelihood that a claim will be of high value therefore putting in to place appropriate control measures to manage the impact of these claims. Precision also empowers insurers to interrogate large amounts of data and turn this into actionable and accurate insights to make informed decisions throughout the claims management process.

Improving processes with fewer resources

Insurers are coming under increased pressure to settle claims quicker, whilst using less resource and reducing overheads. Predictive analytics is now helping our insurance client to not only identify potentially fraudulent claims but also fast track the lower value, genuine claims and allow leave more resource to concentrate on the claims most likely to impact their revenues. The prioritisation of claims via Precision eases workloads, helping to increase efficiencies.

Next steps

The current predictive analytics initiative with our client is nearing completion and implementation. We are excited at the potential this project offers, to help us assist our current and future insurance claims clients. We would be interested in talking to other insurance clients, to see if this new development would help enhance their claims management process.

For more information and to discuss your requirements please contact Osman Khurshid, our Predictive Analytics Business Development Manager on 0333 234 3414.

Is it time for the mobile sector and finance industry to

COLLABORATE

more in the fight against fraud?

With the increasing proliferation of apps within internet enabled devices in the banking, insurance and retail sectors we assess the possibility for network operators to use collaborative fraud prevention systems to prevent smartphones being exploited by fraudsters.

Over the last few years the way in which the consumer accesses the myriad of financial services they need to run their lives has radically changed. Ten years ago most people would have thought it the norm to visit a bank to open an account or apply for loan. At that time the expectation on getting decisions around those loans, mortgages etc. was that the financial institution providing the credit could take a few days to make their decision.

Fast forward to today and the world is a very different place. Today people are rarely visiting their bank branch for any of their banking needs, and decisions across a host of financial services including insurance and banking are expected in a matter of seconds or minutes – even for some of the large scale loans and mortgages that they are applying for.

Additionally in insurance any face to face contact that consumers have with those companies providing their insurance policies has long since become a very distant memory.

The technology that has been the main game-changer for the way that we all purchase our various financial services has been the array of internet enabled devices, such as Smartphones, and the development of online 'apps' has really transformed the relationship people have with their financial service providers.

In fact a recent study by Ernst & Young (EY) showed that three of the UK's biggest banks had over 18 million customers actively using their various banking apps – and that was back in 2017!

On the surface the benefits of migrating services and channelling them through these apps is a win-win for both the companies providing the services, as well as the customers.

The cost savings, marketing opportunities and sheer efficiency inherent in channelling customer interactions and transactions via mobile devices is self-evident. For the customer the sheer convenience of being able to transact, transfer funds, open accounts and buy services all from their phone, wherever they are, is ideal and an obvious choice.

However, issues around data security, privacy and the ever present threat of these devices being abused by criminals means that as mobile devices start to become the predominant way in which financial services are accessed there is the opportunity to improve the way that checks are carried out to prevent fraudsters from so readily abusing these devices.

"Mobile network operators take fraud very seriously and are already working with each other to try and reduce risks."

Currently a key method for checking security for many areas of online transactions is device profiling, and the IP address or profile of a device forms an important part of the KYC journey in many areas of financial transaction authentication.

However, the ability to acquire a mobile device, and therefore download numerous banking or insurance 'apps', is fairly straightforward. Allied to this the acquisition of a no contract, pay as you go smartphone, can be done with minimal checks in place.

This means that financial criminals could, for a fairly minimal investment, access a tool that opens up a whole world of possibility for them. Once one has acquired their 'burner' phone the device initially has a clean IP address, and this means that this device would clear any initial profiling checks. The ability of fraudsters to then use a variety of tactics to socially profile genuine customers, access their various banking or insurance accounts can begin – safe in the knowledge that by linking these profiles to 'clean devices' their chances of successfully avoiding the multi-layered defences of the finance or insurance providers has increased.

"In the United States, anyone purchasing a pre-paid mobile device or SIM card is required to provide identification and their name, home address and date of birth to reduce the risk from the outset."

Another method that could be used to help address these risks would be for the mobile network operators to look at sharing data with other sectors to help mitigate the risks of smartphones being acquired by those with criminal intent.

Today many of the largest network operators already share application data via the Equifax Fraud Exchange. This is primarily used in order to prevent those with a bad credit history from acquiring contract phones. However, the challenge is how to mitigate the risks of these devices being used as a Trojan Horse to undermine the fraud checks that financial services companies have put in place.

EQUIFAX®

Keith McGill, Head of ID & Fraud at Equifax says:

"The Telecoms industry has invested heavily in shoring up their fraud defences in recent years. As fraudsters increasingly target sectors like mobile phones, where they see the checks as being easier to get through, the industry needs to continue looking at new ways to further strengthen their fraud checks."

"Extending out existing data sharing across their peer group to work more collaboratively with other sectors will provide one way to achieve this."

By sharing data with the banking and insurance sector network operators could start to incorporate more sophisticated checks into the process of people acquiring these devices that would enable them to quickly reference fraud data. This would enable them to identify applications that are coming in from known fraudsters.

Given the possibility of real-time responses that are possible these days checks of this kind need not add significant friction to a point of sales transaction, and would help to prevent these powerful devices from being exploited by those with ill-intent.

Based on a recent piece of research conducted by Synectics Solutions there is huge potential to improve identification of those with an 'adverse' fraud history – which if put into a live check could be incredibly valuable in helping to prevent smartphones being abused in the ways mentioned above.

Bringing the Network Operators into greater collaborative data solutions such as National SIRA would effectively plug another important loophole that is available to criminals and create better defences for all of us in the fight against fraud and other financial crime to secure what is rapidly becoming an area of concern.

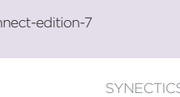
Does your team have the ability to identify and fight complex fraud cases?

ORION

Increasingly, providing a greater proportion of your financial or insurance services online inevitably creates risks, as the lack of physical interaction between lenders, underwriters, and customers creates an environment that organised criminals are actively seeking to exploit.

As a result of this growing trend for organised fraud, prevention systems based solely on the direct matching of individuals are often not capable of spotting the complex, nuanced, and often hidden network of connections that exist between groups of individuals trying to orchestrate fraudulent activities.

Over 50% of insurance claims and policy fraud was of an organised nature for the first half of 2018[1]



76% of fraud committed across all finance products was organised during the first half of 2018[1]

SPOTTING ORGANISED CRIME

Orion from Synectics Solutions was built to specifically address these kinds of challenges by providing a fraud network visualisation and detection platform that puts the kind of analytical and data visualisation capability required to deal with this kind of financial crime, right into the hands of fraud investigation teams.

A senior fraud investigator from one of the largest UK banks discusses how Orion has enabled them to transform their ability to identify and stop organised gangs from impacting their business.

"We've been an Orion user since its inception and it has become a critical part of our fraud detection infrastructure. Essentially Orion provides us with the ability to identify, and therefore counter, complex organised fraud rings that we wouldn't be able to without the network visualisation capabilities that Orion provides to our investigations teams. For example, within the first six months of the system being put live we were able to detect significant fraud activity within our branch networks that we just wouldn't have had visibility of if it wasn't for Orion's network detection capabilities.

The solution has also been particularly useful for our mortgage fraud investigators who have found Orion invaluable when it comes to helping deal with the threat of intermediary based fraud and for detecting unauthorised introducers or ghost broking rings. Through Orion our investigators can easily identify the hidden connections between individuals that exposes their fraudulent activity by trying to hide behind apparently clean intermediaries or by applying through our direct channels.

Now that Synectics have enhanced Orion by allowing it to fully leverage National SIRA data the solution is even more powerful. By widening the intelligence base from which we can draw our network analysis we'll be able to improve our ability to spot patterns of behaviour much sooner – and therefore be able to be more predictive in addressing and preventing organised fraud."

"Organised fraudsters are not brand loyal and often go from lender to lender looking for a way in."

"Having the ability to see the complex links between individuals, which in a traditional data matching solution would be hidden from view, really has seen a fundamental step-change in our ability to successfully combat organised fraud."

1: www.synectics-solutions.com/our-thinking/details/connect-edition-7

Working with trade associations to share knowledge and best practice

As part of our ongoing commitment to collaborative working relationships we regularly engage with a number of industry bodies to promote cross sector knowledge sharing and best practice, when it comes to fraud and financial crime prevention.

Our established relationships allow us to be at the forefront of industry news, trends, events and changes that impact the sectors we operate in, and more importantly our clients. We capitalise on these partnerships to ensure our subject matter experts are best placed to cascade this knowledge, to help you maximise your financial crime strategy.

If you would like to talk to us about our partnerships and the opportunities they present, please speak to your Business Development Manager.

BVRLA

British Vehicle Rental and Leasing Association (BVRLA)

The BVRLA is the UK trade body for companies engaged in vehicle rental, leasing and fleet management. The organisation works with the UK Government, public sector agencies, industry associations and consumer groups to address and remedy technology and finance-related issues.

Synectics Solutions is now a member of the BVRLA with the aim to educate its members on the importance of fraud and financial crime prevention, for motor finance and vehicle rental organisations specifically.

FLA

Finance and Leasing Association (FLA)

The FLA is the leading trade body for asset, consumer and motor finance. In 2017, members of the FLA provided £128 billion of new finance to UK businesses and households. FLA members comprise banks and their subsidiaries, the finance arms of leading retailers and manufacturing companies, and a range of independent firms.

Synectics Solutions has been a member of the FLA since February 2018 and has already been working with other members of the FLA to learn about and help address their challenges when it comes to financial crime.

ABI

Association of British Insurers (ABI)

The ABI is a leading insurance trade body and has over 250 members. It aims to inform and educate its members on policies, regulations, consumer rights and requirements as well as promote the value of insurance.

The ABI's associate membership category has been developed to meet interest from non-insurance companies such as legal firms, consultants, price comparison sites, and the wide variety of suppliers, including software houses, who help insurers deliver their services. Synectics joined the ABI in October 2018.

UK FINANCE

UK Finance

As a key member of UK Finance, we are delighted to be the main sponsor and co-author for this year's UK Finance Economic Crime Academy.

The UK Finance Economic Crime Academy will feature a series of educational training webinars designed to help educate SIRA and UK Finance member on the latest aspects of fraud – with some detailed recommendations as to how these issues can be dealt with and what range of technology and techniques should be considered to be best practice.

Insurance Fraud Bureau

HOW CAN INSURANCE FRAUD BUREAU DATA HELP YOUR BUSINESS?

SYNECTICS SOLUTIONS IS THE FIRST PROVIDER TO BE AWARDED THIRD PARTY SUPPLIER STATUS BY THE INSURANCE FRAUD BUREAU

Now insurance clients, who are also members of the IFB, can now match policy and claims to the IFB intelligence in SIRA to enrich fraud investigations.

IFB Data can help you to:

- Enrich existing data and intelligence to help you make more informed decisions, to mitigate risks quicker.
- This unique data source is currently available via batch processing to allow a more considered and in depth analysis of the intelligence and matches.
- The data can be configured in standard rules and results are displayed in SIRA as part of existing workflows, providing a single view point for matches and investigations.
- Updated bi-weekly, the data is accurate and relevant to guarantee teams have the latest intelligence to make quick, informed decisions and remain compliant.

Find how to access Insurance Fraud Bureau Data in SIRA. Call us on 0333 234 3417 or 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

AR