CallValidate.
An unrivalled suite of verification.

Bank
- Bank Account Validation
- Account linked to Name & Address
- Direct Debit Setup
- Validate Non-Consented Bank Accounts
- Bank Account Plus

Identity
- ID Verification
- Impersonation Checks
- Date of Birth Validation
- Knowledge Based Authentication
- Comply with AML Regs
- Age Verification
- Employee Vetting
- CallValidate 3D

Card
- Card Validation
- Card Linked to Name & Address
- Card Details Validated
- Payment Validation
- Card Enhanced

International
- Global ID Verification
- Global Passport Verification
- ID Card Verification
- 135 Countries On-line
- Web and Integrated Service

Fraud
- Ownership Fraud Alert
- Velocity Checks
- Real-Time Fraud Alerts
- Delivery Fraud
- National Change of Address
- Fraud Database
- Over 70 Configurable Fraud Checks Delivered

To find out more:
- enquiries@callcreditgroup.com
- www.callcredit.co.uk/callvalidate
- 0113 388 4300
Callcredit’s Fraud & ID business has grown significantly in recent years, driven by continual development of some of the most innovative Fraud & ID solutions available that provide enhanced levels of trust and pinpoint risk across the customer lifecycle. Our focus is on creating a frictionless customer journey for genuine customers whilst identifying fraud risk accurately.

Consumer behaviour has changed in recent years, the way firms and consumers interact has changed, digital channels and in particular the mobile channel is becoming increasingly the preferred option for consumers. And in the same way that consumers have fuelled innovation in terms of faster, more convenient ways to interact across most sectors (for example mobile payments), its also fuelled our approach to developing new innovative solutions to provide trust in those interactions.

The move of consumers to the on-line channels is being driven by the ability to do things faster, more cost effectively, with more choice, at any time and from anywhere. Consumer behaviour is further supplemented by initiatives such as the Government’s ‘Digital by Default’ programme which is aiming to drive consumers to the digital channels to interact with government.

This means that establishing trust and digital identity is becoming increasingly important and the absence of a single universally accepted method of identifying consumers in the UK will fuel even further innovation in the coming years. Callcredit are at the forefront of driving this innovation, already developing new solutions that do not solely rely on personal identity trust solutions, but also incorporate non-personal identity attributes and behavioural methods to achieve trust.

Identity has evolved significantly, new technology and the amount of data generated by individuals has increased dramatically which presents both challenges and opportunities for our customers. Consumers are starting to take more control of their data, using it to make their on-line experiences more beneficial and personalised to them. Taking control of our identity and how, when and why it is used is a natural progression in this evolution. Callcredit are committed to establishing increased levels of trust for consumers.

I hope you enjoy the views and comments expressed within this report.
The Challenges Today

Today’s society is largely characterised by rapid advances in technology. From Instagram and iPhones, to Google Glass and Driverless cars, the way in which we interact with technology in our everyday lives is developing at a phenomenal rate.

The proliferation of the internet, and more sophisticated every-day electronic items have all added a new dimension to the nature of and the types of fraud being committed. With more information being stored electronically this in itself creates more opportunities for the fraudster to target information that can then be used to commit a wide spectrum of fraud. Consequently the fight against the fraudster is an ever changing landscape with new technologies constantly being updated and reviewed to respond to the ever-growing and evolving nature of this threat.

The Trust Continuum

In order for us to be best placed to combat the risk of fraud we need to evolve the way in which we look to tackle the associated components of fraud.

Historically fraud detection methods have concentrated on primarily name and address validation however today we must also look at aspects of non-personal trust and risk solutions. When our clients interact with their customers they now want to establish trust but also at the same time identify the risks too – both of which could be considered closely aligned but the extremes of which and the consequences of their abuse are quite distinct.

What is the problem we are trying to solve?

For the growing number of organisations that are highly reliant on the use of digital channels the challenges they face are increasing particularly when looking at areas associated with fraud and identity.

The Challenges

- A change to the verification methods that can be used effectively. Less use of face-to-face checks and physical documentation, and more use of non-personal identity data such as data relating to ‘devices’ and behaviours.
- Increase in fraud from professional, organised gangs.
- Globalisation of the source of these threats – organisations can be attacked from anywhere.
- Increasing access by criminals to a market in compromised identities and credentials for sale, with which to perpetrate fraud.
- More opportunities for criminals to impersonate identities as services are originated and delivered online (therefore more value in fraudsters developing a fake or impersonated identity).
- Increased regulation on the checks that organisations need to carry out with the potential to adversely impact service delivery and customer satisfaction.
So what is driving this increase in risk?

There is no doubt that verification needs and requirements are changing particularly with the rise of online and mobile transactions. Ultimately the pressure is being placed on organisations as the end consumer, you and I, have become accustomed to being able access products and services almost instantly. A perfect example of this is how historically we would have applied for a personal loan, filled in an application form possibly a face to face meeting with a representative from the lender following which, if approved the funds would be transferred in to your account in a day or so – somewhat of a lengthy process. Today in most cases this is an automated process often with funds transferred in to our account sometimes in minutes – a process that is also convenient to the fraudster.

More organisations are encouraging account openings and origination online. There is a continued rise in online purchases together driven in part by mobile payments through services like Zapp, Paym and Monitise. Increasingly organisations are providing services directly via Apps which in themselves provide a perfect opportunity for the fraudsters to access a vast array of services such as bank accounts providing they have the right level of personal information. Consequently as a business it’s important that we are able to respond and deliver the right technology to respond to these challenges - example include:

- On download of an App it’s crucial to able to establish a “Triangle of Trust” between the client, the device and the services they use.
- This ‘Trust’ is then used to provide higher risk services and access to confidential information.
- There is a significant risk that it may not be the true customer downloading the App.
- Banks are seeing more impersonation attempts at point of download of an App.
- At Callcredit we can help establish that the download is to the actual customer’s phone.

The future of fraud mitigation is in the ability to leverage frictionless techniques, along with a multi-layered and multi-dimensional approach that will achieve a strong authentication. Big Data can offer big protection in helping to fight fraud through real-time, event driven behaviour analytics creating a wide range of ‘trust and risk’ solutions

At Callcredit we have an intelligent suite of fraud solutions but we are not ‘resting on our laurels’ - far from it. We are always looking to broaden the depth and breadth of our solutions, looking at ways in which we can harness new innovative technology that will deliver cutting edge fraud solutions that will help both our clients and their customers combat fraud not just now but also in the future.
In 2013 the level of insurance fraud hit a record £1.3bn, according to the Association of British Insurers (ABI) an increase of 18% on the previous year. The biggest rise was in car insurance. The number of identified dishonest motor claims increased by 34% to 59,900 an attempt to cheat the industry out of £811m.

One of the issues faced by the insurance industry is fraud manifests itself in many different ways ranging from dummy insurance, impersonation fraud, ‘fronting’, ‘Crash for Cash’ to application fraud. Whilst some acts of fraud are perpetuated by organised criminal gangs who look to commit premeditated fraud others are carried out by individuals whose motivation is driven by external pressures such as the rising in cost of living, downward pressure on income and increased levels of personal debt. The challenge for the industry is to try and implement solutions that can identify fraud whether premeditated and opportunistic.

At Callcredit we work with some of the biggest insurers in the insurance industry such as Aviva and Allianz to help improve their understanding of risk and to help strengthen their fraud awareness. Our fraud and risk tools are designed to be used at every stage of the customer lifecycle. Uses include providing greater insight at the ‘Customer Acquisition’ stage during and particularly at the crucial payment stage. Our tools can also be used for ‘Customer Management’ and claims management or even when there is a need to verify identity associated with a proposed high risk or a significant claims settlement.

Our CallID tool is an ID verification process which provides robust confirmation of the policyholder’s details and provides a clear indication of any instances of data being fabricated from a wide variety of sources. One of the key features is that we are able to provide address links which can highlight instances where adverse information, such as previous claims experience or repudiated claims being concealed at a previous address.

Our searches are run against a wide variety of both positive and negative datasets including the Electoral Roll (ER), updated annually and monthly from local UK authorities and containing over 45m UK adult names and addresses.

Through products provided within our flagship ID verification tool ‘CallValidate’ we can offer bank account verification – ownership fraud alerts – we can identify if a bank account doesn’t belong to the applicant, and with ownership fraud alert we can return the name of the person it actually belongs to. This is extremely useful when verifying account details at point of claim when a settlement has been made and the insurer is looking to process the payment.

CallValidate can also be used to ensure that the presented card details are valid and that they can be linked to the given name and address. If the card details cannot be linked to the given name and address, CallValidate will attempt to identify who the owner of the card is. In addition CallValidate has the facility to conduct a live check on the card verifying that the card is active and so not blocked, or reported lost or stolen. We can see how many times a card has been used in a defined period of time, and we can also see if it has been supplied with a variety of personal details, flagging any inconsistency in the data provided.

All of which help insurers to identify the ‘tell-tale’ signs of potential fraudulent activity. The overarching message is clear - Insurers need to ensure that they respond to the challenges of the increasing sophisticated techniques used by the fraudsters by implementing robust, flexible fraud detection measurers. Our technology is specifically designed to be adaptable to the ever changing threats.
A successful response?
Detected fraud continues to rise with just under 120,000 fraudsters identified last year alone. We also now have much stronger claims and underwriting fraud controls in place combined with stronger collaboration with organisations such as the Insurance Fraud Bureau, City of London Police and Cheatline – but more does need to be done.

So why have consumer attitudes not changed?
In essence the overriding issue is that we have failed to create any tangible consequence to committing acts of insurance fraud. We need to make it much harder for identified fraudsters to obtain insurance and other financial services. For those who have been convicted of fraud we have to make it even more difficult for them to obtain insurance. The cost of future insurance needs to be much more expensive with a similar stance adopted by insurers as that for convicted drink drivers. Sentencing guidelines for convicted fraudsters also need to be increased, historically sentences of eight years were common place but today the maximum sentence being handed down by the courts is on average only three years.

Collaboration – How does this all fit together?
ABI - Association British Insurers – Financial Crime Committee – made up of a ‘technical board’ (fraud experts), Supervisory Board (CEO level) and ‘management board’ (fraud experts).
IFB – Insurance Fraud Bureau – takes all shared insurance data, motor policy database, personal lines database – to identify those who have been unlucky and what we want to pick out is those individuals who have been involved in far too many accidents in far too shorter time.
IFR – Insurance Fraud Register – black list of fraudsters – set up to share information both within the industry and outside. It is expected to be used by insurers at pre-quote stage which will enable insurers, for the first time, to say “we don’t want to deal with you”.
IFED – Insurance Fraud Department (part of City of London Police) a specialist unit dedicated to tackling insurance fraud and is committed to addressing high volume and organised criminality in collaboration with justice partners, has helped but more needs to be done - it’s only a small force tackling a national problem.

Cheatline – a phone line created for people to report incidents of suspected fraud - operated by Crimestoppers is now taking 500 calls a month.
Each element of this collaboration framework plays an important part whether its detection, prevention, response and importantly prosecution. It also has to include effective control mechanisms, which is why it’s important to have the buy-in from industry CEO’s.
A big challenge, similar to that faced by other sectors, is conduct risk. What must be avoided is data leakage which will simply render the process ineffective, a situation that can be compounded when organisations sitting outside industry governance look for ways to supply and sell data to us.

Maintaining integrity:
A key element of our future fight against the fraudster is the effectiveness of the implementation of the ‘Insurance Fraud Register’. Launched in December 2013 to date there have been 93 expressions of interest together with 54 ABI members wishing to join the scheme in order to share the data. it has strict loading criteria; data refreshed every seven days, individuals actually advised of breach of a policy fraud condition, a robust definition of fraud and data only deleted after five years, which represents a severe sanction even for the small discretions. This information will also be shared with banks, building societies and HMRC which will ensure that future access to financial services becomes increasingly difficult for the fraudster.

The next phase – widening access:
For it to be a real success the data contained within the IFR needs to be shared with whoever wants to share it. The benefits will be far reaching and will demonstrate collective action, increased front-end capability, will provide a platform for brokers, aggregators, non ABI members and will establish links to other sectors.
What is needed is a real change in consumer attitudes where acts of fraud will no longer be tolerated and the consequences harsh.
The gaming industry continues to evolve thanks to the fundamental shift in how consumers engage with gaming services through mobile and tablet devices, as online gaming becomes a more socially acceptable leisure activity. As a direct result of this change in player behaviour the industry is seeing an increase in regulatory requirements in order to protect both players and operators alike.

New regulations, such as the 4th EU Money Laundering Directive will challenge operators to obtain a more in-depth view of their customers to prevent potential fraud and money-laundering, not only at the inception stage but throughout the whole customer lifecycle.

Gaming operators as a standard procedure already have a number of automated checks in place to quickly and efficiently check a customer’s name, address and date of birth. Many also have additional checks to verify that the payment method, be it card or bank account, being used by the customer to fund the account, is owned by that customer and therefore helping to prevent identity fraud, payment fraud, unauthorised withdrawals, account takeover and money laundering.

Despite the extent of this verification process there have been a number of cases brought to light which support the need to undertake enhanced due diligence checks, ensuring that the operator has a deeper knowledge of its customers and their circumstances.

There have been a number of high profile cases highlighted in the industry recently, which have resulted in an increased requirement for additional verification. In some cases, individuals have been found to be gambling well outside of their means, utilising funds from sources such as stolen goods.

While these individuals will have passed the relevant ID requirements and the payment method will have been verified, the value and volume of bets made should have been a cause for concern and further investigation. After reviewing the cases the Gambling Commission concluded that there was too much over-reliance on third parties such as the banks and their AML processes and not enough use of external data sources as actively as there could have been. Additional data, such as income and expenditure information could have been used to manage any potential risk, and to identify money laundering or problem gambling.

While some cases may have seemed extreme, they were unfortunately not seen in isolation and the regulatory environment reflects this. As such, in the future we will now begin to see operators not only using credit data alone to mitigate risk, but also incorporating consumer insight data to build a deeper picture of their customer’s lifestyle and status to help undertake enhanced due diligence checks.
These cases have highlighted the need for operators to have a more in-depth view of consumers across multiple aspects. New regulations will require more insight into things such as income risk, investments, property details, length of residency and employment to name but a few.

Currently the majority of these additional checks involve a series of manual investigations into each customer by operators, which can be a lengthy process. Subsequently, we’re progressively seeing more operators coming to Callcredit seeking further insight and data which they can stream-line into their existing processes to reduce the time spent undertaking these.

By using databases such as our customer segmentation tool CAMEO and consumer database Define it is possible to better understand their customer’s lifestyle, their demographics, their behaviours online and offline, as well as confirming any significant life events. All of which can be used alongside modelling techniques to identify risk behaviour patterns which may be indicative of financial crime.

If operators had previously had access to consumer insight data at the point of application, they would have been able to gain a view of any potential fraudster’s means; what sort of property did they live in? Where the size and frequency of their bets in line with their lifestyle? Likewise, by using additional data in this way it’s possible to identify if an individual’s gaming behaviour suddenly changes or falls outside of the expected behaviours, this could flag with the operator that there could be a problem and further investigation can be undertaken.

Using data in this way has been highly successful in other sectors. For example, utility companies use behavioural data to determine cross-sell opportunities and risk management strategies, and perhaps the most relevant - the alternative finance sector, which similarly to the gaming industry, has seen an increase in regulations and the need for deeper customer insight to make more informed decisions to diminish risk.

The growing pressures of the regulatory environment mean that operators will need to be more proactive in identifying and managing potential risk going forwards and should therefore make use of all the data that is available to them. By incorporating customer insight datasets alongside existing fraud and risk strategies operators will have a more granular view of their customers, with increased automation and efficiency, which is of critical importance to the gaming industry.

<table>
<thead>
<tr>
<th>Marketing Data</th>
<th>ID Verification Data</th>
<th>Credit Risk Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAMEO - Individual, Household</td>
<td>CallValidate search data</td>
<td>Bureau Summary Block - Summarised credit report data</td>
</tr>
<tr>
<td>and Postcode data split into 10</td>
<td>Gives a view of the level of identity data held for an</td>
<td>for an individual to give a view of their current</td>
</tr>
<tr>
<td>different CAMEO groups</td>
<td>individual together with a series of decision warning</td>
<td>credit risk profile.</td>
</tr>
<tr>
<td>Provides an in depth view of</td>
<td>messages around residency, impersonation fraud and</td>
<td></td>
</tr>
<tr>
<td>consumers across multiple</td>
<td>identity risk.</td>
<td></td>
</tr>
<tr>
<td>aspects from income risk,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>investments, property details,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>length of residency,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>employment plus many more.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
As we move into an increasingly cyber world, consumer attitudes to how we take control of our personal data are rapidly changing. In this digital age we no longer rely on a locked filing cabinet to hold our most sensitive documents or a photo album to hold our memories. Instead we are choosing to store this information digitally, in emails, on hard drives and now in the cloud.

While this makes it easier than ever before for consumers to access and control their personal data it also brings with it a new kind of fraudster; a kind that is not only illusive, but are experts in organising well-engineered and meticulously executed operations to obtain our personal details.

In recent years the media have increasingly reported on large data breaches from some of the world’s largest and most trusted organisations. Where once these attacks may have been aimed primarily at banks and financial institutions, criminals are now targeting any company that may hold a myriad of data on us - from tech and gaming companies even your local supermarket.

Until recently it might have been considered the ‘norm’ that these organisations rather than individuals should be responsible for keeping personal information safe. While this is still absolutely the case, consumers are now realising they too share a responsibility in keeping their own data safe. As such, we’re starting to see a two-pronged approach between the consumer and the industry with both parties working to together to thwart criminal activity.

At Callcredit we’re not only working hard in key markets to help protect consumer data, but we’re also helping to lead a major change in the consumers’ attitude to their own data and how they can access it. With our free-for-life credit reporting service Noddle we’ve empowered over 900,000 UK consumers to take charge of their identity and financial history. As a credit report is one of the first places the signs of identity fraud may appear, consumers can easily keep a watching brief on their own identities.

Even though we are seeing Noddle going from strength to strength, we’re also seeing a healthy demand for our other credit checking services. We recently rebranded the service now known as ‘Credit Compass’ and it was launched in early February, together with our updated £2 statutory report service, completing the full suite of facilities that we offer consumers – which supports the fact that consumers are starting to take more control of their finances and are becoming much more vigilant.

As with any consumer product, it’s important to recognise that one size doesn’t fit all and evidently different consumers have different needs, with this in mind we will continue to offer consumers choice in which service they want to use, rather than pushing everyone down the same route.
As well as empowerment of the consumer, we must also strive to improve our collective understanding of exactly how and where our own personal data might end up, particularly when shared through the wider use of social media, and identify what new methods criminals might use to access it and exploit it.

The UK’s fraud prevention service CIFAS recently found that in the first three quarters of 2014 almost half of all confirmed fraud in the UK was identity fraud. However, cases of recorded identity fraud are down slightly on previous years and part of the reason for this is the growth in public awareness.

As a population we’re now generating and sharing more information than ever. We’re freely distributing our personal details in return for free services and with the advent of the selfie and social media we’re willingly offering up our personal lives to the internet, often without thought of potential consequences.

We live in an age of increasingly instant gratification where things like loss of internet connection or a delayed delivery is unacceptable. This attitude drives innovation in consumer services, but it also means we may be less inclined to question things or look beneath the surface when trying out new applications. In 2010, the High Street chain Gamestation added a prank clause to their T&Cs which saw thousands of their customers legally handing over ‘the right to their souls’! This served to highlight what we as consumers can often sign up for without realising it.

A recent 2014 survey found that 73 percent of us still never bother to read the T&Cs or fine print when signing up to a new service or app - an attitude that criminals can and do seize on. By creating slick looking apps and services which often look just like legitimate ones we may be inclined to download or try them without further question often providing too much personal information.

Despite this relatively recent uplift in technologically fraudulent behaviour the basic rules of consumer fraud remain the same, if something looks too good to be true then it probably is. But learning to spot that in a world that’s always aiming to please is a big ask which is why consumers and organisations need to work together to tackle fraud in a fast moving digital age.
Looking to the future - increasing our capability

In January 2014 Callcredit announced the acquisition of analytical software solutions and consultancy provider Coactiva, an acquisition designed to further extend the range of innovative products and services we could offer to the public sector. Coactiva is a pioneer in bringing sophisticated, innovative ‘Big Data’ Analytics & Business Intelligence solutions into everyday use within many public sector organisations. With market leading solutions Coactiva enables organisations to reduce costs, increase revenue and improve service through the use of risk-based analytics. Coactiva also provides market leading performance management software to over 23,000 users across the UK, which includes 1800 educational establishments, 130 local authorities and organisations within social housing, the emergency services, health and leisure.

The acquisition of Coactiva further demonstrates Callcredit’s continued commitment and enthusiasm to develop its Public Sector business. Callcredit has enjoyed significant success and growth since its inception three years ago and the acquisition reflects its ambition for the sector. The addition of Coactiva’s cloud-based performance management software and risk based tools adds expertise, depth and a further dimension to the range of products and services it is able to offer new and existing clients in both the public and private sector.

One of the on-going challenges faced by the public sector is the continual battle with spending cuts, policy changes and the fight against fraud, whilst at the same time striking a balance on how best to help protect the public purse.

The theft of taxpayers’ money has a direct impact on reducing the resources that can be spent on frontline services. Every pound stolen from government means that there is less to spend on health, education, policing and defence. Reducing fraud is also a matter of fairness: every false benefit claim reduces the amount available to those deserving of government support and every false tax return means that more money needs to be raised from the honest citizen. In the current economic environment, losses due to fraud are even more unacceptable. As the public sector is forced to cut back spending, tackling fraud effectively offers an efficient way to achieve the Government’s number one priority of reducing the deficit.

A collaborative approach

Government departments need to adopt a collaborative approach where good practice and intelligence are shared freely in order to combat fraud. Departments such as HMRC and DWP have led the way, developing considerable expertise in preventing, detecting and investigating fraud – but this expertise needs to be shared more widely.

Local authorities also need to adopt a common approach to tackle the specific fraud threats they face collectively. For local authorities in particular one of the main challenges is how to combat tenancy fraud. Latest figures from the annual fraud indicator estimate that the annual cost of tenancy fraud to local authorities is £845m and
£919m via housing associations. Research undertaken by Callcredit highlighted that over 80% of local authorities still don't have a dedicated fraud team in place.

The Group is well placed to understand these challenges having seen its footprint within the sector grow extensively over recent years. In response to this we continually look for ways in which we can change our products and services in order to make them fit perfectly with the demands of the industry and has a comprehensive range of solutions aligned with the Government’s Fraud, Error and Debt strategy. As with all types of public sector fraud, the key to tackling it is to understand the scale of the problem and the inherent risk, work to prevent fraudulent activity occurring and put in place a zero tolerance approach to dealing with identified cases.

One significant change we have helped implement is the greater sharing of information between local authorities. As a result of which we have brought together 16 London Borough Councils to establish a ‘Fraud Hub’, with a further 4 councils also sets to join, called the ‘ThreeSixty Hub’. The Hub not only allows local councils to share data between each other but Coactiva is also able to help match their data with its own extensive data sets – helping to provide greater insight and in turn help target fraudsters more effectively, saving time and money. We have already seen some significant results as a consequence of the ‘ThreeSixty Hub’ being formed and our plan is to use this as a ‘blueprint’ to establish other similar models across the UK.

By sharing data, knowledge and adopting a more collaborative approach with neighbouring authorities, housing associations and where applicable, central government departments, local authorities can work to reduce the risk of tenancy fraud and increase the detection rate.

Coactiva has, for the last 8 years, been the UK’s leading provider of Risk Based Verification solutions which prevents Housing Benefit Fraud from entering the system.

Delivering Innovation

Effective use of data is the key to both identifying fraud and preventing fraud. Coactiva works with a number of organisations from across the public sector in helping to tackle and eradicate fraud, types of fraud that can affect both organisations and individuals alike. One example is the way in which Coactiva has been working with Royal Mail.

Royal Mail wanted to drive the profitable growth of its online postal Redirection service, take on more legitimate customers, increase efficiency and save money. As part of Royal Mail’s drive it wanted to ensure no corresponding increase in fraudulent ‘Redirections’ or identity theft occurred. Royal mail required a robust identity verification (IDV) solution and as such Coactiva has provided its market leading, online real time identification solution - CallValidate.

CallValidate enables Royal Mail to validate and identify over 90% of legitimate customers in real time, and enables lower failure rates with people gaining, and paying for the ‘Redirection’ service they want in one, straight-through application. In addition, for any customers who’s application failed – perhaps as a result of their payment card being registered to their new address – Coactiva provided a knowledge based authentication channel, CallValidate 3D, driving ‘Redirection’ revenues whilst maintaining strong anti-fraud measures.

Through the use of CallValidate and CallValidate 3D Callcredit was able to assist Royal Mail with the following challenges:

- Driving growth – successfully identified more applicants
- Preventing fraud – stop fraudulent ‘Redirections’
- Saving money – moving applications online
- Improving the customer journey
- Delivering innovation – continuous improvement and best practice

As a direct consequence Royal Mail saw the following results, 4% uplift on pass rates compared to Royal Mail’s previous supplier of IDV services, a further 4% uplift through the use of CallValidate 3D and an enhanced customer application process, helping Royal Mail drive its online channel.

“Coactiva fully understood our specific online authentication needs and provided a solution which increased our redirection application pass rate with no negative impact on fraud. This has successfully been expanded with additional knowledge based authentication to further drive volume and revenue.”

Andrea Martin, MD Royal Mail Data Services
Software development and leading edge analytics are two competencies consistently highlighted as our key points of difference. In our tenth customer satisfaction survey conducted in June 2014 it confirmed that:

- 97 per cent of clients would consider the company for future projects
- 91 per cent confirmed that Callcredit provided quality, accurate credit data/intelligence/solutions, which enable companies to better understand both their existing and potential customer base
- 81 per cent said Callcredit had a strong reputation.

We are constantly reminded that the world is continually changing being driven by technology-savvy consumers who are becoming accustomed to receiving products and services in a real-time environment. In parallel with this advancement there is a need to ensure that consumers and businesses alike have the confidence and reassurance that they have adequate systems in place which keep up to date with the advancement in new technology.

Earlier this year CIG announced the creation of a new division designed to expand the capabilities of the Group specifically focusing on Software, Analytics and Fraud and which also includes the unique multi-bureau capability of DecisionMetrics.

DecisionMetrics recently launched its latest and most sophisticated version of ‘DecisionStrategy’, a next generation decision engine that offers the highest levels of flexibility in strategy configuration and change. The new functionality includes a work flow module, ability to assign work queues with diary functions, data input and underwriting screens, a bureau independent credit data viewer and multiple duplicate checking options. This means that in addition to automated decisioning, any difficult cases that need manual intervention can be allocated to a specific work queue e.g. fraud, so that an expert can work the case off-line.

DecisionStrategy was already unique in the marketplace with the inclusion of DecisionMetrics’ multi-bureau technology and its Strategy Control System that allows the business user to configure the decisioning logic including the process flow, scorecards, policy rules, terms of business and when to request data from internal or external data sources including credit bureaux. This latest generation of the product can now deliver end to end sophisticated application processing, but can also be configured for non-credit decisioning functions such as fraud and collections.

The product continues to evolve and will be looking to include more innovative modules and functionality to allow an increasingly sophisticated end user access to the latest tools and techniques.

The creation of the new division will ensure that the Callcredit Group continues to been seen as market leaders in this space and will enable the business to provide the correct level of strategic focus required to grow our capability both organically and through acquisition. As our analytics, software and fraud propositions continue to grow and gain traction within the market the creation of the new division is a timely reminder of our commitment to our existing customer base and new markets.
INTEGRATION OF SIRA AND CALLCREDIT SERVICES PROVIDES A REAL-TIME CAPABILITY TO HIGHLIGHT FRAUD AND CREDIT RISK FACTORS THROUGH A SINGLE, INTEGRATED RISK MANAGEMENT SYSTEM ELIMINATING THE NEED FOR DISPARATE SOLUTIONS, INCREASING OPERATIONAL EFFICIENCIES AND SIMPLIFYING IMPLEMENTATIONS

Jona Aucott, Head of Sales and Product at Synectics Solutions

PARTNERSHIPS
BY KERRY CLEARY Solutions Analyst – Fraud & ID

Working together and in good company
Fraud continues to be a rapidly growing area of our business which now accounts for approximately 15% of the group revenue. This is a significant growth area for the business as our clients look to us to expand and enhance our services in this area.

We have been working on several new initiatives to help to meet our client needs, as well as partnering with leading ‘blue-chip’ companies. Key partnerships within fraud and prevention include working with companies like Featurespace, Iovation and Synectic Solutions.

Featurespace
Callcredit has partnered with behavioural analytics specialists Featurespace. The partnership provides Callcredit with access to Featurespace’s core Adaptive Behavioural Analytics engine – ARIC, and its team of data scientists, as well as providing a secure experience for consumers and merchants using mobile payments. The ARIC engine combines the power of Bayesian statistical algorithms with advanced machine learning to create the only Adaptive Behavioural Analytics software in existence.

This ensures that Callcredit’s unrivalled data assets are combined with the world’s most advanced approach to data analytics, enabling Callcredit and its clients to remain at the forefront of machine learning technology. The partnership will enable Callcredit to develop new innovative solutions as a result of ARIC’s ability to understand individual and group behaviour in real time calculating human interaction events before they occur.

Martina King, CEO of Featurespace said: “The ARIC engine enables clients to understand the positive and negative behaviour of their customers. Our solutions range from the most up-to-date fraud identification, to churn predictors and customer analysis. Combining Callcredit’s impressive data sets with our unique analytical approach has created a truly innovative partnership. Data is set to become one of the most valuable commodities this century, but it’s what we do with it that will create the real value.”

Iovation
Callcredit has also entered into a strategic partnership with Iovation, the trusted source for mobile and online fraud prevention to safeguard businesses. The partnership combines complementary data and technology to deliver market-leading fraud prevention and identity solutions. The partnership, which builds on an existing relationship created in 2011 between Callcredit and Iovation will bring about a new era of combined device and bureau-based data solutions. The agreement will expand and strengthen Callcredit’s fraud and verification suite with Iovation’s device intelligence and device reputation manager.

Scott Olson, VP of Product for Iovation, commented, “Iovation stops Internet fraud and identifies good online customers by leveraging the world’s largest device reputation database. Our abilities to uniquely recognise devices, comment on their history of fraud and abuse, identify associations to other risky devices, and reveal data anomalies provide a strong and complementary defence to the robust identity and fraud protection offered by Callcredit. We are pleased to have joined forces with Callcredit in the fight against fraud.”

Synectics
Synectics Solutions, founded in 1992, is an independent data management company who specialise in providing managed service solutions for the detection and prevention of fraud for both the public and private sectors. Callcredit and Synectics Solutions have had a successful partnership since 2007, enabling centralised intelligence by combining Callcredit’s ID & fraud capabilities with SIRA, Synectic’s industry leading fraud detection and prevention solution.

SIRA was built using feedback from risk and fraud professionals, designed to provide a scalable and customisable fraud prevention platform, offering full lifecycle protection across financial services and insurance markets. The solution caters for the ability to match data against national syndicated fraud intelligence, the capability to leverage best-in-breed data sources within a sophisticated decisioning and workflow engine, along with overarching network analytics and case management technology.
The latest figures from Financial Fraud Action UK reveal that both card fraud and remote banking fraud are on the rise during the first half of 2014. As more and more of our day to day spending continues to move into the digital space these figures should come as no surprise. However, with this move to the digital channels comes the increased risk of customers leaving themselves open to malware, phishing and card data compromise.

Card not present fraud has been a challenge for the UK Banking sector for a number of years with one of the more common card not present fraud themes being the fraudulent use of card details to undertake low value test transactions such as mobile phone top ups, charity donations and music downloads. However, there are now so many compromised cards in existence, the details of each card are cheaper for fraudsters to buy and so the fraudsters no longer have a need to perform these test transactions on cards to establish if the details are still active – instead the cards are being used for single, higher value transactions which in turn is driving higher card not present losses in the industry.

What can we do?

Customer education remains a key priority for many organisations, looking to protect their customers from the many deception methods employed by fraudsters. However, despite numerous campaigns to remind customers of the importance of being vigilant whilst interacting online, we still see alarming numbers of customers not taking the necessary steps to ensure their identity is safe whilst online. A recent survey by Cyber Streetwise found that 75% of people surveyed admitted to not following best practice guidance to create complex passwords and 35% of those questioned admitted that they did not create complex passwords as they struggle to recall them.

Typically when a customer forgets a password to access an account or undertake a transaction online they will be taken through a password reset process. This will be based on the input of static data which in itself is often easily accessible to a fraudster or is information a fraudster can find out by undertaking a little research.

A move away from the Password?

With this in mind, organisations in the financial services sector are now turning their attention to alternative methods of establishing trust and identifying risk. We've already seen moves away from a purely static authentication approach where the only defence is a password entered by a customer to more dynamic authentication such as one time passwords towards two factor authentication.

These measures, coupled with the capture of more granular device and customer data are just the starting point to ensuring that as we accelerate further into this digital age, fraud losses don't increase at the same level.
CallValidate.
An unrivalled suite of verification.

**IDENTITY VERIFICATION & VALIDATION**
Callcredit’s wide range of quality robust data sources enables a menu of identity verification solutions to be deployed within CallValidate. From a simple confirmation of name and address to a more complex Anti Money Laundering ID check or Knowledge Based Authentication solution, our customers are in complete control of the level of identity checks they deploy.

**BANK**
CallValidate Bank Solutions provide increasing levels of verification of bank details. Simply validate a bank account is valid or prove it belongs to a name and address, the solution can be configured to your requirements. CallValidate can uniquely return matches on ‘non-consented’ bank accounts and reveal the true owner’s identity if it is not the name and address supplied.

**CARD**
CallValidate Card Solutions uniquely verifies that card details are valid, correct and linked to the name and address supplied. If the card cannot be linked to the presented name and address, CallValidate returns the details of the true owner of the card. CallValidate is connected to the live payment network and instantly verifies if a card is active, blocked, lost or stolen.

**FRAUD**
Delivering over 70 configurable fraud warnings in a single instant check, CallValidate enables you to pin point fraud accurately whilst improving genuine customer pass rates. Each Fraud Prevention module can be switched on or off within CallValidate and configured to optimise your fraud prevention strategy.

**INTERNATIONAL**
CallValidate International verifies name, address and date of birth from over 135 countries worldwide. Further countries are due to be released soon along with enhanced fraud prevention capability.

To find out more: enquiries@callcreditgroup.com
0113 388 4300
www.callcredit.co.uk/callvalidate
Helping you to solve the crime of Public Sector fraud with Coactiva

£14bn
Tax fraud

£2.5bn
Central Government fraud

£2.2bn
Local Gov. fraud
£90m
Single Person Discount Fraud
£1.2m
Housing Benefit Fraud

£1.6bn
Benefits & Credits fraud

50,000
Social Homes are Unlawfully Occupied

£20.3bn
Of public sector fraud

THE CRIME

ThreeSixty
EMPTY HOMES
Enables councils to establish if a home is empty and, where applicable, take advantage of the New Homes Bonus.

ThreeSixty
TENANT VIEW
Monitors existing tenants for change of circumstance and prevents fraudulent applications and allocations.

Case Report
STOKE-ON-TRENT
Recovered £3 additional properties that were subject to fraud as a direct result of the Coactiva project. A saving of £14,000.

Case Report
ORBIT SOUTH
Has prevented £1 million in tenancy fraud.

Case Report
RBV
DWP approved on-line Risk Based Verification service enabling Local Authorities to detect fraud and error in benefit claims.

Case Report
HUB
Saves Local Authorities access to housing benefit, social, tenancy and waiting list info. Allowing members to determine if tenants are claiming housing benefit elsewhere.

Case Report
NORTH WEST METROPOLITAN BOROUGH COUNCIL
Out of 28,000 individuals claiming SPD Coactiva found 804 potentially fraudulent cases. Additional income recovered: £149,000.

Case Report
NORTHAMPTON BOROUGH COUNCIL
Tenant View helped recover 15 social homes that were subject to tenancy fraud. Each property was worth approx. £130,000.

To solve the crime, phone: 0345 279 7250
email: contactus@coactiva.com or visit: www.coactiva.com