ISSUE 5 / WINTER 2011

Creditlines

Supporting success through continued IT investment

In this edition

Callcredit
Information Group

Supporting success through continued IT investment

STRUCTURE

Over the last five years Callcredit Information Group has seen significant levels of growth both organically and through acquisition. It has consolidated its place as an industry leader in its chosen markets and has a recognised brand that reflects the organisations approach to innovation, flexibility to client requirements and high quality service. Callcredit is committed to keeping pace with client requirements and exceeding expectations with regards to the performance and availability of its services, in particular constantly improving its supporting technology and hosting infrastructure. Callcredit recognises that the scale of growth achieved over recent years requires us to take a different approach in how we structure ourselves to deliver our current and future promises. The time is now right to create a fully integrated operating environment that provides a comprehensive shared service capability across all businesses within the group.

We have implemented a new internal structure over recent months to address this creating a specialisation focus across all our IT functions.

SECURITY

As custodians of our clients' data and information relating to UK consumers, this places us in a privileged position and therefore information security is vital in providing both consumers and our clients with the right levels of data and access integrity confidence. As such we continue to invest in the expertise within our Information Security team to support the increased focus we place on all security controls and monitoring.

DELIVERY

We have invested heavily during 2011 in additional people within Delivery to ensure that we have the skills and expertise to match the pace of growth that Callcredit continues to achieve. We are strengthening Service Management Capability to support our service delivery ensuring that the Callcredit Group not only develops strong innovative products but that these are operationally supported and maintained meeting service level agreements with clients and are fit for purpose. Callcredit acknowledges that service delivery is the foundation stone of its success and a great differentiator in a competitive industry.

PROGRAMME MANAGEMENT

In a fast paced business whose reputation is built upon innovation and agility we need to ensure we can continue to positively respond to customer demands for new or enhanced product opportunities. We have recognised the importance of this by creating a Programme Director role which is focused on prioritising delivery of all of our products and services across the Group, Implementing an agile framework centred around Dynamic Systems Development Methodology (DSDM).

This edition of Creditlines is focussed on enabling smarter decisions relating to financial crime and fraud across a number of sectors including Insurance, Financial Services and Gaming. Our continued IT investment supports innovation for our customers within their current and new processes, providing new insight into fraud challenges and solutions.

If you would like further information contact:

Adrian Mitri
Chief Operating Officer
E: adrian.mitri@callcreditgroup.com
or call: 0113 244 1555

Rising to the fraud challenge

Callcredit's 5th Annual Financial Crime Conference was held earlier this year at the Wellcome Centre in London.

For the 2nd year running I had the pleasure to chair the event which is now in its 5th year and continues to attract a great deal of interest from financial crime prevention professionals. Once again, interest in the event was high and delegate numbers were significantly up on previous years which is encouraging to know the event is well received.

After 4 years of holding the event at the Institute of Engineering and Technology, this year's event moved to The Wellcome Centre due to the increased numbers of attendees and accessibility of the venue. However the venue was not the only change, this year saw a change to the format too with the event being split into two themed sessions:

Session 1 – Where have we come from?

The first session was aimed at looking back over the 5 years since our event began with a look at the scale of fraud in the UK and how it has changed, highlighting trends in the way fraud has been committed.

Opening Remarks
John Cannon, Head of Product Strategy, Callcredit

The opening remarks included a look at the economy and its effect on fraud over the last 5 years, a specific look at the growth in ID Fraud in recent times including a look back in history at famous cases that highlight the fact it is not a new phenomena. The opening remarks also included a general update on Callcredit since the conferences began and a summary of some key product developments for fraud prevention.

Fraud in the UK
Matt Allan, Head of Strategy and Policy, National Fraud Authority

Matt provided an overview of the current fraud landscape in the UK, how it has changed over the last 5 years and provided a summary of the work the National Fraud Authority are engaged in to help reduce fraud in the UK. One such example was the NFA's Information Sharing Taskforce that has a number of aims including facilitation of better data sharing between public and private sectors.

Fraud: A Banker's Perspective
Mark Tingey, Head of Fraud Prevention, Royal Bank of Scotland

Mark provided an interesting insight into fraud in the banking sector and how it has evolved over the years paying particular attention to 1st party, 2nd party and 3rd party fraud. The session also focused on the globalisation of fraud in recent years and how RBS strike the right balance to reduce fraud losses.

Session 2 – Where are we heading?

The second session was aimed at looking forward at new trends in fraud and new technology to combat it.

Uncovering Hidden Fraud Networks –
George Robbins, Head of UK Markets, Detica

George provided a look at fraud networks including the evolution of risk systems and the rise of fraud analytics. A comparison of people's views towards fraud in different countries and a fascinating case study showing the movement of fraud between organisations after the adoption of fraud prevention technology.

Buyer Beware – Building Trust
Tom Ilube, Managing Director – Consumer Markets, Callcredit

Tom provided an entertaining perspective on fraud by concentrating on the consumer's view and how we can all play a part in stopping fraud. Tom also announced the launch of Noddle.co.uk, Callcredit's new consumer web site offering consumers access to their credit report free of charge for life.

e-Signature: New Risks, New Solutions
Abe Smith, Director, IOCS

Abe provided a glimpse into the future and the use of digital signatures which are becoming more and more popular in the credit industry as a way of electronically signing credit agreements. He provided detail on US legislation and how that could impact the UK in the future.

Feedback from the event was once again extremely positive for both the speaker's content and delivery which made for an interesting and entertaining event. The conference was followed by a drinks reception which I'm told carried on late into the night! I'd like to thank all the speakers for the effort they put in to make the event a success, I'd also like to thank the delegates for joining us at the event, we look forward to seeing you again next year.

> "I was delighted to contribute to what was a very worthwhile & successful event."

Mark Tingey,
Head of Fraud Prevention, Royal Bank of Scotland

> "The Callcredit Financial Crime Seminar was informative, well-organised, and a great networking opportunity. I plan to attend again in the future"

Kevin Braden
Manager, Risk Mgmt & Fraud Prevention, Enova Financial

John Cannon
Head of Product Strategy, Financial Crime
E: john.cannon@callcreditgroup.com
07872 808 207

To pre-register for 2012 Annual Fraud Conference, email marketing@callcreditgroup.com

Fraud prevention with pin point precision

Callcredit launch Ownership Fraud Alert

Ownership Fraud Alert (OFA) is one of the most exiting innovations in ID and payment fraud prevention in recent years. Delivered as an additional service through our flagship fraud prevention product, CallValidate, OFA has increased the number of CallValidate fraud warnings and enables our customers to pin point fraud at point of application or during payment transactions.

CallValidate combines traditional electronic verification of identity with the unique ability to verify card and bank accounts are owned by that identity. It achieves this through cross referencing of the card number, bank account and sort code with Callcredit's SHARE database.OFA has been developed to detect and prevent ID and payment fraud by pin pointing applications and transactions where the identity presented with the card or bank account does not own it.OFA fraud warnings will tell you the name and/or postcode of the person who is registered to the card with pin point accuracy.

"We are consistently finding new ways to improve our products and services and the development of OFA will have significant benefit to the full range of Callcredit customers. Financial institutions will use it to verify individuals at the point of application whereas retail and gaming clients, will use it to authenticate online transactions and reduce chargeback's.

OFA is just one of over 70 sophisticated fraud warnings within CallValidate that can be configured to be in line with our customer's business strategy."

John Cannon

OFA has been designed to return manageable referral rates with low false positive rates enabling you to deploy your optimal fraud prevention strategy for ID and Payment Fraud. This extra insight closes the loop on fraud and the combined wide range of configurable verification and fraud checks gives you unrivalled power in detecting and preventing fraud.

If you would like further information about Ownership Fraud Alert or CallValidate contact:

John Cannon
Head of Product Strategy, Financial Crime
E: John.cannon@callcreditgroup.com
or call: 0113 244 1555

Occupancy fraud a concern for insurers

Over the last few years we have witnessed significant changes in the mortgage market in terms of the volume of mortgages, value of mortgages and product type availability. There was an overall decrease in the number of mortgages made available by lenders, a decrease in the value of mortgages, reductions in the maximum amount loaned against property values and tightening of lending criteria such as increased credit scoring acceptance levels. In addition, a number of mortgage lenders withdrew from the market. The cumulative effect of these changes made it difficult for many people to obtain a mortgage product than at any time in recent years.

Mortgage products most significantly affected during this period included sub-prime mortgages, self-certified mortgages and buy-to-let mortgages. According to the Council of Mortgage Lenders (CML), in 2009 there were 93,500 buy-to-let loans advanced; compared with 222,700 advanced in 2008, representing a year on year reduction of 58%. The value of buy-to-let mortgages in 2009 was £8.5billion compared with £27.2billion in 2008 and whilst 2010 and 2011 has witnessed some recovery in the market, the buy to let mortgage market is currently still running at a third of the levels seen in 2007.

Logic suggests that as it becomes more difficult to obtain a mortgage product, we could expect to see increases in first-party mortgage fraud, however this theory does not manifest itself solely in relation to mortgages it can be applied much more widely across most types of fraud associated with financial lending products including insurers. Occupancy fraud is causing concern to mortgage lenders as a direct result of the reduction in buy-to-let mortgage products and home insurance providers should share that concern.

Occupancy fraud occurs when a borrower obtains a mortgage on a property with the intention to rent out the property, but declares on the application form that the borrower will occupy the property as their main residence. The aim of the borrower is to obtain a lower interest rate associated to a homeowner occupier mortgage and avoid paying the higher interest rates generally associated with buy-to- let mortgages. In addition the borrower is also likely to disclose to the prospective home insurer that the insurance required is for a normal homeowner occupier therefore negating the need for the insurer to attach the higher premium associated with that of a rental property. Alternatively the insurer in question may choose to not even provide cover for a property offered for rent and under normal circumstances re-direct the property owner to a specialist insurer.

Non-owner occupier properties historically have higher delinquency rates and this increased risk represents one of the reasons for the higher interest rates and insurance premiums charged. In the case of occupancy fraud, both lenders and insurers are left overexposed and, as a result, lend larger amounts or higher loan to value rates then they would normally for buy-to-lets with insurers specifically exposed as they currently receive a premium that is not commensurate with the risk .

However the occurrence of occupancy fraud is not restricted to the point of application. The combination of changes to the borrower's financial circumstances (brought on by changes to the economy, reduction in property value and reduced prospect of selling their property) is forcing many homeowners to rent out their homes while living with family or friends. Many of whom do so with little or no regard for the change in the physical risk type but more importantly some do so completely unaware of what the consequences of their actions might be.

Failure to disclose the fact that a property is rented out to an insurer could render the insurance policy void which if only identified at the time of a loss could provide grounds for the insurer to repudiate the claim - consequently leaving the property owner exposed to the possible potential of losing everything.

Failure to declare the change in circumstances to a lender is classed as a form of occupancy fraud as the borrower is required to obtain a 'consent to lease' under the existing homeowner occupier mortgage or to be transferred to a buy-to-let Mortgage: both of which command premiums from the mortgage lender and the insurance company.

Occupancy fraud is illegal. The property owner is deliberately misrepresenting the risk in order to obtain more favourable terms. In addition, the property owner may also be perpetrating tax fraud by not declaring the rental income gained on the property.

Occupancy fraud has traditionally been virtually impossible to detect, unless the property owner admits to renting out their property. Callcredit has engaged with a number of financial service providers to understand fully the issue of occupancy fraud and, as result, has developed a highly effective strategy to uncover and detect property owners who are currently renting out their property. Callcredit's 'Hidden Lets' solution uses a range of powerful databases, including bureau data, to piece together vital information about the policyholder. Hidden Lets evidences the presence of multiple mortgages, links to other addresses and the presence of recent tenant verification checks carried out at the property address.

John Cannon
Head of Product Strategy, Financial Crime
E: John.cannon@callcreditgroup.com
or call: 0113 244 1555

Consumer attitudes to Insurance Fraud

“we are all victims of insurance fraud”

“my premiums just increase”

“Scammer”

“hey they can afford it”

Outside of the industry, insurance fraud is often referred to as a ‘victimless crime’. As such, the common perception is that it is acceptable behaviour, and something that in one form or another is perpetrated by a significant proportion of the population.

On the face of it, the argument has a ring of truth. In many peoples’ eyes, the only real victims are the insurance companies, and the typical consumer view is “hey, they can afford it”. However, for example, research shows that around £50 of the cost of a motor insurance policy goes towards subsidising fraudulent claims and uninsured drivers. Ultimately then, far from being victimless, insurance fraud is a crime which affects everyone in the shape of increased premiums.

In a survey carried out by Callcredit (YouGov April 2011), 61% of 45 – 54 year olds and 34% of 18 – 24 year olds highlighted that the impact of ‘knowingly over-inflating an insurance claim’ affected consumers the most. This clearly indicates that there is an acceptance that acts of fraud in the insurance sector do have an impact and yet the general view is that it is still deemed as acceptable behaviour.

Whilst a variety of insurance frauds, ranging from simple over-inflating a sum insured to organised crime rings, have been relatively commonplace for many years, acts of first party fraud have seen a dramatic increase in recent times. This is primarily due to the ability to purchase products online. Our research showed that 63% of 18 – 24 year olds and 54% of 35 – 44 year olds said ‘online’ was the easiest way to provide inaccurate details to purchase goods and services from insurers. This compared with only 8% and 3% respectively for face-to-face transactions.

Clearly a distinction needs to be made between what are ‘opportunistic acts’ and pre-meditated crimes committed by organised fraudsters. Insurers can tackle both by implementing a wider use of more sophisticated fraud identification tools. However, in order to challenge the belief that insurance fraud is acceptable, insurers’ need to understand the motivation behind consumers’ behaviour.

An issue that insurers often face is that the customer judges them on how good (or bad) they are when it comes to dealing with claims. The common perception is that insurers are quick to accept business and increase premiums, yet slow to respond when it comes to paying out. Unfortunately, this is a view which can breed mistrust and animosity, which in turn leads to the justification and motivation for fraud. Surprisingly, when asked about circumstances in which it would be acceptable to inflate an insurance claim, 12% of 18-24 year olds confirmed it would be ok if the insurer delivered poor customer service.

Insurers need to respond to these challenges by putting in place robust fraud detection measurers at both the application and claims stage. Our research suggests a direct correlation between the propensity to submit fraudulent claims and a customer’s credit history, as well as whether or not their details have been validated. However, few UK insurers choose to use full credit data checks; a practice used widely in the United States.

As insurance frauds become more sophisticated, the need to implement robust defences increases. Insurers have the ability to deploy a range of solutions which include credit checking, verifying ID, matching identity to the payment details, and tracking velocity. Embracing new technology will enable insurers to react quicker, while failure to act could leave them exposed and vulnerable to fraudsters.

If you would like further information contact us:

Graham Odiam
Head of Sales – Insurance
E: graham.odiam@callcreditgroup.com
or call: 0113 244 1555

Changing attitudes to first party insurance fraud

Finding the right balance between fraud prevention and good customer experience is a challenge for all consumer facing businesses. Insurers are seeing increasing pressure to address this challenge as the way we interact with customers becomes faster, more remote and by different channels such as price comparison sites. So how do we address the problem of ensuring we are not exposed to increased fraud risks whilst addressing the need to maintain good levels of customer experience?

As fraud becomes even more prevalent it is crucial to understand the difference between legitimate changes to the proposed request and those changes that constitute a false declaration. It's very easy to keep changing the details on an application in order to try and secure a lower premium, whilst sitting at home with a laptop submitting quotes to a price comparison site. Some of this will be genuine, such as adding named drivers or adjusting the level of excess for example, whilst some will be fraudulent (changing your DOB, postcode, address etc) and for every quote submitted via a price comparison site a large number of insurers will respond with a quote.

Insurers are also conscious of providing customers with the most competitive premium without them having to go through a lengthy time consuming process, as customers will often choose to terminate and insure elsewhere. Insurers are therefore motivated to provide 'best' rate and then validate the customer application details prior to committing to commence the policy. Historically the focus has been on getting new business volume on the books and less on the quality of risk which led to insurers having to allocate resource to fraud detection at the 'back end' as opposed to detection at the 'front end'. Hence there was often conflict between marketing departments chasing volume and underwriting departments chasing quality risks. The suggestion is not to decide between validation at quote rather than claim, but simply to consider a more balanced approach.

Most insurers only use public data and transactional data but the use of velocity checks can help to identify first party fraud more effectively. For example, high volumes of transactional data at one address or postcode can help to identify those cases of organised fraud rings emanating from one address.

The implementation of velocity checks at the application stage has often been avoided due to the need for major and lengthy IT projects being required to integrate such a solution into legacy systems.

The benefits to insurers of using multiple verification criteria at application stage are proven by the fact that Callcredit have found instances where the average claims value is 70% higher for a customer that has not been verified by name, address and DOB.

Insurers need to recognise the value first party fraud identification tools can make to the overall performance of their book and that there has to be a trade off between speed of quote and the acquisition of better quality risks. Failure to do so will ultimately make it easier for the fraudster and will increase their exposure to poor risks.

Results show that for those who choose to use first party fraud tools there is an improvement in the quality of risk taken on and therefore create an opportunity to better focus investigation resource when claims are received. And of course, for those who embrace this early and make the right investment in the right areas will be those who benefit the most as fraudsters move on to others with a less robust process.

If you would like further information contact us:

John Cannon
Head of Product Strategy, Financial Crime
E: John.cannon@callcreditgroup.com
or call: 0113 244 1555

Data driven fraud identification

Earlier this year The National Fraud Authority published its annual fraud indicator for 2011 and estimated a mortgage fraud loss figure of circa £1 billion for 2011. In an environment where the majority of mortgage lenders are being very risk averse this represented an ever increasing percentage of the advances being made.

Callcredit, having access to its unique data set about looking at how to assist their clients in this challenging arena.

A recent study carried out for a large mortgage lender initially looked at deriving maximum value from Callcredit's SHARE database using complex address matching techniques to identify applicants with 'undeclared' addresses. By looking for both forward address links as well as undeclared addresses, numerous alternative links were identified. A significant percentage of these applicants had been passed by the mortgage provider's underwriting team and were found to have insolvencies, defaults or county court judgements registered at an address they had not divulged to the mortgage provider.

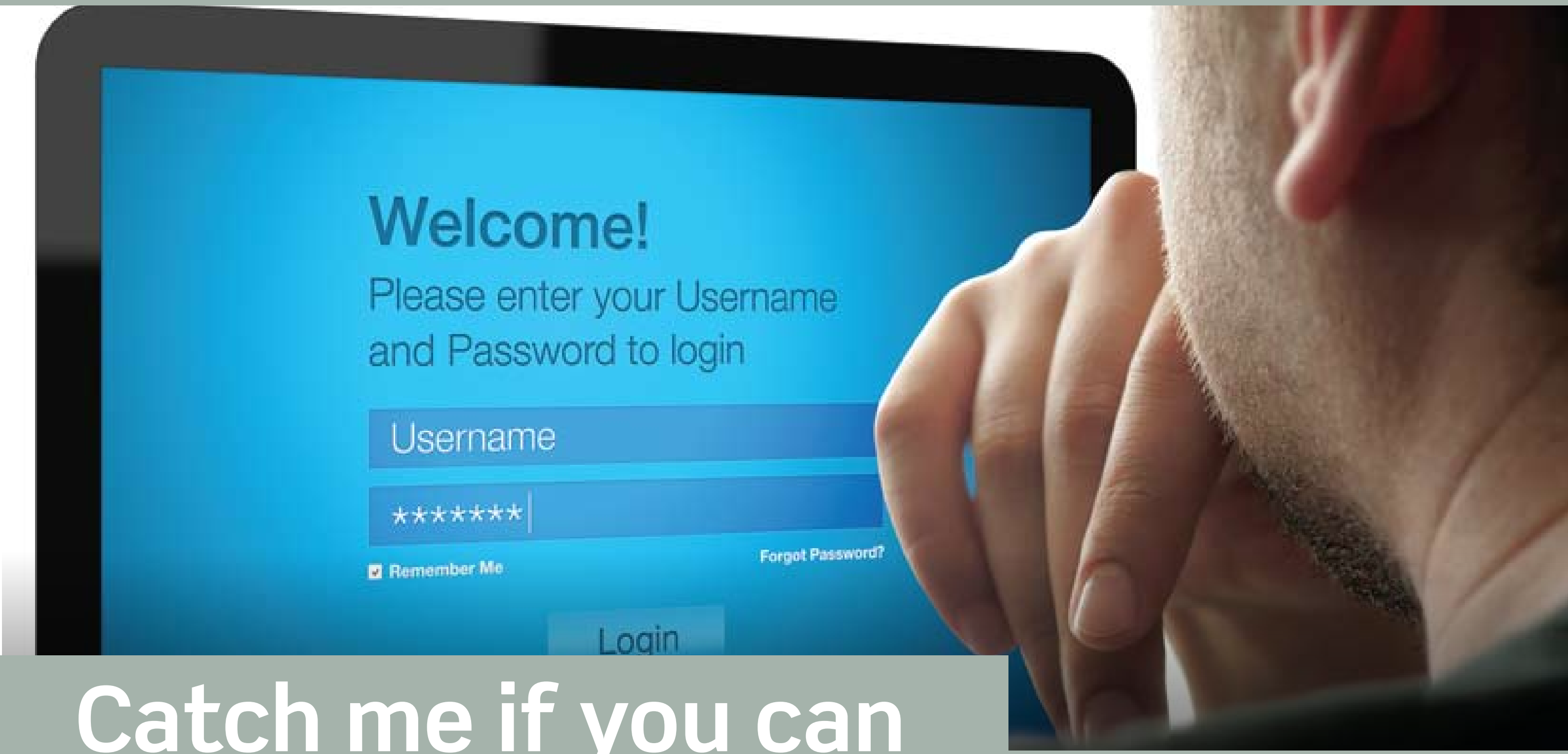
Operationally, these applications should be declined or referred out to an investigation team and having removed them the second stage was to investigate the applicant's financial associates. Applications in a single name can be a sign of someone trying to hide negative information about a partner. A further significant amount of the remaining applications had serious derogatory information registered against someone associated to the applicant but not disclosed at the time of application.

Remaining applications were then investigated using a combination of the more traditional identification and verification solutions and the data contained within Callcredit's Over-indebtedness Initiative database. The value added by these products identified where an applicant, or a broker/ introducer, had inflated an income given on an application by comparing the details given to those held within the database. The combined power of these datasets identified more potential fraudulent applicants whilst simultaneously reducing the false positive rates.

Any of the individual data sets taken in isolation can, and do, add value to a fraud investigation, whether the delivery of the data is direct into a client's fraud system or via a third party software provider. However, the maximum value is derived by engaging Callcredit's consultancy and analytics experts to develop a bespoke set of rules and delivering a more informed data driven decision.

If you would like to find out more about how Callcredit's fraud consultancy and analytics team could help your business reduce fraud and improve customer acquisition contact:

Mick Ellender
Head of Consultancy
E: mick.ellender@callcreditgroup.com
or call: 0113 244 1555



Catch me if you can

Impersonation fraud is not a new phenomena, if you look back in history you will find many examples of Impersonation fraud. 'Princess Caraboo' a book by John Wells, was based on a true story from 1817 of a disorientated young woman who was found wandering the streets speaking a foreign language and claiming to be a Princess from the island of Javasu in the Indian Ocean. She claimed to have been captured by Pirates and jumped overboard in the Bristol Channel and swam to shore. She was treated like royalty by locals until her cover was eventually blown and she was unmasked as a poor cobbler's daughter from Devon.

The 2002 Stephen Spielberg's blockbuster movie 'Catch me if you can' was based on the life of serial impersonation fraudster Frank Abagnale Jr, who carried out cheque fraud by impersonating occupations such as airline pilots, doctors and lawyers. In 2001, Karl Power managed to join the Manchester United team before their Champions League game with Bayern Munich, successfully posing as team member Eric Cantona for their pre match team photo.

In each of these cases, the fraudster displayed the unwavering characteristic of confidence to be able to pull off the fraud. The need to show complete self belief to make others also believe in the fraud is not something the majority of us would be able to achieve. However the modern ways we do business with consumers and the need to make interactions faster and more remote present highly attractive opportunities to carry out impersonation fraud. No longer does a fraudster have to adopt a high risk impersonation strategy such as those used by Frank Abagnale Jr, these days it can all be done electronically from the safety of your home and enables the fraudster to detach any emotion from the criminal act.

As consumers, we demand that our interactions with service providers (e.g. banks, credit card companies, retailers, insurers etc) require as little interaction from us as possible. The requirement for us to carry out actions such as visiting a branch to present documents to verify our identity and prove we are who we say is generally viewed as a hassle.

As a result, more and more firms are looking to adopt paperless straight through processing of customers, therefore causing them least intrusion without becoming an easy target for impersonation fraud. At Callcredit, we spent time asking our customers what they wanted from impersonation checks and three characteristics were fed back in virtually every case:

1) The check should be instant and available 24/7

2) The check should provide a high confidence level that the person is who they say they are and therefore stop fraud

3) The check should not cause additional intrusion on the customer – therefore does not impact on the customer experience and satisfaction

If you could remove this type of fraud, imagine the effect it would have on your business? The savings could be used to develop new products, win more customers through marketing, improve customer satisfaction or simply recognise it to your bottom line.

Based on this customer feedback, Callcredit have enhanced CallValidate to meet these requirements for anti impersonation.

To find out more contact your business development manager or client manager.

John Cannon
Head of Product Strategy, Financial Crime
E: john.cannon@callcreditgroup.com
or call: 0113 244 1555

Fighting fraud in the gaming sector

There are a number of forms of fraud now affecting the eGaming sector, some more specific to the sector than others and some which are commonly seen across a range of different sectors.

The common forms of fraud experienced by eGaming companies include ID fraud, account takeover, under age gaming, payment fraud (for example the use of stolen cards to load a gaming account), bonus abuse and the risk of staff fraud. The sector is also subject to more specific serious organised forms of fraud such as betting rings, insider fraud and money laundering. Fraudsters are also using more sophisticated techniques such as phishing to obtain personal information with a view to taking the victims account over or using malicious software such as Trojans or Malware.

ID fraud particularly is on the increase both within the gaming sector and elsewhere as fraudsters now become more sophisticated in the methods they use. Impersonation fraud is not new phenomena however the way we interact with customers' today demands faster, more remote transactions which present highly attractive opportunities for impersonation fraud.

Consequently it is now more important than ever that operators' within the gaming sector have robust fraud detection tools at their disposal which will determine whether a customer is genuine and that any card they choose to use is verified against the user. Callcredit has developed a unique and highly innovative fraud prevention tool (CallValidate) that provides certainty in matching a customer's name, address and DOB to the 16 digit payment card number or 8 digit bank account they use to load their account or withdraw funds to in one quick operation. In addition, CallValidate can also provide total certainty when the payment card or bank account presented is not linked to the customer by returning the surname and postcode of the person the card or bank account is linked to which can help in the fight against ID Fraud, payment fraud, withdrawal of funds from gaming accounts, account takeover and money laundering.

New forms of fraud

One of the emerging fraud challenges faced by the gaming sector is the increasing growth in the use of mobile gaming. As more and more consumers begin to interact electronically 'on the move' so does the risk of fraud. Operators need to ensure that they have robust checks in place to validate the person using the electronic device, the payment method/type and to be able to differentiate whether the consumer is communicating verbally or electronically via their mobile device.

Increasingly the sector is also being targeted by 'gaming cheats' who use fraudulent identities to avoid being identified as individuals who may have appeared on operators banned lists. Being able to identify these individuals', using velocity checks which indentify multiple applicants, makes sure that every person you have registered is only registered with you once as opposed to the same person in ten different guises – stopping the cheats coming back to you again and again.

Addressing charge-back

Chargebacks in Gaming are equivalent to other sectors and in fact lower than certain sectors such as retail. However all operators experience first-party and impersonation fraud, and, in some cases, stolen and cloned card details are used to deposit and wager on poker sites, with the fraudster deliberately losing to one person. However all operators experience 1st party and impersonation fraud and in some cases stolen and cloned cards details are used to deposit and wager on Poker sites, with the fraudster deliberately losing to one person.

The introduction of 3D Secure software such as Verified by Visa and Mastercard Securecode within most payment channels has helped to reduce the number of chargebacks and fraud in the on-line sector, however it should be noted that 3DS is intended to be used to complement existing fraud checks and should not be used alone to prevent fraud.

The attraction of using 3D Secure is the shift of liability on chargebacks and fraud to the issuer from the gaming company, however the process of forcing a customer through potential additional security screens can lower the overall customer experience and increase dropout rates, something that has been addressed more in recent years.

eGaming companies that choose to rely solely on 3D Secue software alone to cover chargebacks and fraud may find that their authorisation rates from issuers decrease as a result. Any eGaming company who causes higher levels of chargebacks and fraud to an issuer is likely to be considered a higher risk and could result in a stricter scorecard being adopted by issuers. In extreme cases where levels of fraud and chargebacks are very high, issuers have the power to revoke liability and push it back to the merchant. A combined approach of adopting sophisticated fraud prevention solutions with 3DSecure is more sensible approach.

New emerging technologies

In a fast changing world where would be fraudsters are becoming ever more sophisticated in the ways in which they try to mastermind fraud it is imperative that those who might targeted, such as those within the gaming sector, stay one step ahead of the fraudster.

Callcredit has developed a range of products designed to help the gaming sector reduce fraud such as CallValidate which validates a customer's identity and uniquely links it to credit/debit cards and bank accounts of that individual so you can be satisfied that you are dealing with a genuine customer using their own payment details together with over 70 fraud checks that can be configured to ensure you don't cause legitimate, good and honest customers unnecessary inconvenience.

Our latest development within CallValidate proposition is 'Ownership Fraud Alert' which feeds back a range of fraud warnings about the ownership of the card such as highlighting the occasions when the card belongs to a different identity at a different address to the one presented with the transaction.

John Cannon
Head of Product Strategy, Financial Crime
E: john.cannon@callcreditgroup.com
or call: 0113 244 1555

If you would like further information contact us:

Gavin Wright
Business Development Manager
E: gavin.wright@callcreditgroup.com
or call: 0113 244 1555

CIFAS Transformation Project

The CIFAS Transformation Programme has given Callcredit the opportunity to vastly improve the way that CIFAS data is matched and delivered to CIFAS members as part of Callcredit's online and batch services. Ultimately the project will result in members seeing improved fraud detection processes, reduced false positive rates and increases in customer satisfaction.

In simple terms the new targeted approach will reduce the time members spend investigating fraud referrals and therefore reduce associated operational costs and the number of good customers who are referred by a CIFAS match. The resulting improved customer experience can lead to better customer retention and increased customer sales.

Callcredit has committed to make the CIFAS Transformation Programme as painless as possible for members who utilise Callcredit's online and batch services by providing a tiered approach to the new service. Firstly, the existing CIFAS matching service will remain in place until the end of 2011. Our Client Management Team will make direct contact with each member to discuss options before proceeding to change their configuration to the new service. For most members this will result in no change to the service they receive from Callcredit and members will not be required to upgrade connections or screens. This will mean a member using a historic integrated link to access bureau data can switch to using the new CIFAS + service with no change to the output they receive from Callcredit, resulting in no IT work for the member.

If members are able to upgrade connections, it will enable them to make use of more functionality and data Callcredit are making available as part of the CIFAS Transformation Programme.

In addition, Callcredit are providing a fully configurable service to CIFAS members who wish to be selective of the Data Matching Rules they want to implement and this will be hosted in Callcredit's IT environment.

The first of Callcredit's products to go live with CIFAS+ was CallMonitor in July 2010. More recently Callcredit launched CallReport 7.1 which enables clients to make use of the new Data Matching Rules.

To find out more about the CIFAS Transformation project and how it effects your business contact:

Laura Barley
Head of Client Services, Callcredit
E: laura.barley@callcreditgoup.com
or call 0113 244 1555

Callcredit trekkers raise over £13,000 for charity

Employees and clients of Callcredit Information Group took on the colossal Oxfam Trailtrekker challenge, tackling a gruelling 30-hour, 100km trek across the Yorkshire Dales to raise a fantastic £13,400 for Oxfam on June 4th-5th.

28 took on the 'Trailtrekker' challenge on behalf of Callcredit, walking through gale force winds, rain, darkness and exhaustion to raise as much money as possible. Despite injuries and fatigue all walkers covered a huge distance with eight achieving the amazing feat of reaching the finish line in the 30-hour target time.

The Callcredit trekkers have raised £13,400 for Oxfam, with donations continuing to pour in as colleagues, friends and family hear about the unbelievable challenges and achievements of the event. The money will support Oxfam's work in relieving poverty and suffering in the UK as well as around the world.

Mike Davies, Business Development Director at Callcredit said:

"We always expected this event to be a huge challenge, and it didn't let us down! The terrain and weather combined with the darkness overnight and exhaustion really put us to the test, but I am extremely proud of how every one of the walkers did. Raising more than £13,000 for Oxfam really makes the hard work worthwhile."

Donations can still be made to support the Callcredit Trailtrekkers can be made online by visiting: **www.justgiving.com/teams/callcredit-trailtrekker/**

Last year Callcredit colleagues and clients cycled across England in the Coast to Coast challenge and raised more than £8,000 for NSPCC.

Callcredit Information Group Key Contacts

Eamonn Tierney
Business Development Director
eamonn.tierney@callcreditgroup.com
0113 244 1555
07768 977 863

Mike Davies
Business Development & Sales Director
mike.davies@callcreditgroup.com
0113 244 1555
07711 851 222

Graham Lund
Managing Director, Credit Solutions
Callcredit Information Group
graham.lund@callcreditgroup.com
0113 244 1555
07764 268 674

John McAndrew
CEO
Callcredit Information Group
john.mcandrew@callcreditgroup.com
0113 244 1555

Jan Smith
Industry Relations Director
jan.smith@callcreditgroup.com
0113 244 1555
07912 120 994

Adrian Mitri
Chief Operating Officer
adrian.mitri@callcreditgroup.com
0113 244 1555
07881 833 757

Chris Savage
Managing Director, Marketing Solutions
chris.savage@callcreditgroup.com
0113 244 1555
07710 901 671

Tom Ilube
Managing Director, Consumer Markets
tom.ilube@callcreditgroup.com
+44 (0) 754 0702 330

David Swift
Marketing Director
david.swift@callcreditgroup.com
0113 244 1555
07921 883 619