

MEETING MINUTES: SAFER HIRING 17th January 2024

Chair's Introduction: The Chair welcomed the speakers and commented that so much had been learnt from speakers in previous meetings.

Present: Emma Hardy MP, (Chair), Lord Lucas of Crudwell, James Morris MP, Andrew Henderson (Secretariat), Keith Rosser & George Warrington, Better Hiring Institute; (see list at end)

Speakers:

1) Keith Rosser, Reed Screening, Better Hiring Institute Investors in People:

Evolution of what we call hiring fraud, aided by new technology, we are seeing a scaling up of abuses. This is both for employers and work seekers. Keith reminded us of the previous meetings and forthcoming ones.

The Better Hiring Charter has been the outcome of these meetings. The Charter is all about how to reduce barriers to getting into work. As we make hiring faster and fairer those types of change create new problems, hence the inclusion of "safer" alongside faster and fairer. Today therefore we are going to look at hiring fraud.

Previously it has not been looked at in the round, more in a piecemeal fashion. Want to make this the start of the first UK guide to tackling fraud for employers and employees.

What is hiring fraud? Fraud that has an impact on employers and job seekers. It has become more sophisticated with the use of tech and especially AI. We are aware that fraudsters are working in cahoots to offer a paid for service for fraudulent CVs. Also the deception that happens to work seekers and leads them into harm. This is the source of much modern slavery or debt bondage.

Types of hiring fraud:

- 1) Reference houses, we have identified dozens of these in the UK. They pretend to be a genuine business and offer a false reference for a work seeker. To the employer this looks like a genuine business with a level of sophistication unseen before.
- 2) Tech drives hiring fraud. We see the good and bad of AI. We will deal with this in a virtual event in April. Used to unfairly help people get jobs e.g. using Chat GPT to answers online questionnaires. We are also seeing deep fakes and video technology.
- 3) Seeing the scaling of the problem with scams aimed at work seekers. BBC has covered fraud a lot recently, 30% of UK adults have experienced a scam. 7 in 10 WhatsApp users have received fake job offers.

We are seeing sophistication but why does it matters?

Safeguarding problems as those not qualified get a job in healthcare, education etc. Also about safeguarding customers such as when visiting a bank. There is a link between organised crime and employment as they seek to get people placed in organisations.



MEETING MINUTES: SAFER HIRING 17th January 2024

For victims, the experience can set them back both in time and money through fake job offers. Sorting out hiring fraud will help productivity in the UK .

Important to stop worker abuse such as non-payment by an agency or modern slavery. If we sort this out then there are lots of benefits. The toolkit will help businesses to help themselves. By writing the first guide to tackling fraud we can equip employers with the right tools. As a call to action would like all of us here to help. We have seen this drive in fraud and in sophistication. For under £150 I can get a fake birth certificate, I can get a fake NI card or bank statement to support my employment history. These systems are intelligent.

2) Alison McDowell, Beruku

Hiring is changing. The use of technology and AI opens up a range of potential improvements that enhance the quality of our hiring practice and is also opens up risk from those who intend to perpetrate wrongful and criminal deception for their own financial or otherwise personal gain and gratification.

People who perpetrate fraud and abuse tend to zone in on what they regard as 'easy targets'. This can be children and young people and adults with care and support needs – and that means all of us at some time or another as we all have care and support needs, even if it's temporary, at different points in our lives.

The Care Act 2014 describes 'financial abuse' as a type of abuse which includes having money or other property stolen, being defrauded, being put under pressure in relation to money or other property and having money or other property misused.

So fraud is abuse and can happen in any sector that interacts with the public including banking, retail, education, law, criminal justice, health and social care.

People impacted by fraud and any type of deception suffer very real harm not just in a material sense, but emotionally and psychologically. In this way, fraud is a safeguarding issue.

When talking about safeguarding, we are often referring very specifically to the protection and promotion of welfare of children and adults at risk of abuse. However, we can also apply a wider definition that encapsulates public protection more generally. You can see from the work of BHI that it deals with both ends of the spectrum from children and adults at risk of abuse, the key focus of the Better Hiring Toolkit, and in the support of the JobsAware campaign regarding job scammers.

If we apply a safeguarding lens to hiring and fraud in hiring, what do we see? Safeguarding has always been and will always be a hugely dynamic environment. Abuse and prevention of abuse is a socially constructed phenomenon that depends on a particular place, at a particular time, in a particular culture. Abusers and fraudsters might be using different techniques to target their victims and perpetrate their crimes, but their motives are largely the same – personal gain and gratification. Harold Shipman falsified prescriptions, Ian Huntley used a different name, Lucy Letby fooled everyone that she was a good nurse and Jimmy Savile used the power of celebrity



MEETING MINUTES: SAFER HIRING 17th January 2024

to gain access to hundreds of children and adults at risk. It's the same bad actors with the same motivation posing the same risks using different techniques and methods.

Likewise, people have always used a variety of tools and methods to measure and mitigate the risk of harm and articulate what has to happen to prevent it. There are always children and adults at risk, vulnerable groups, who can be targeted through all sectors.

So, we see the same types of people looking for the same gain and gratification but using different techniques.

The techniques fraudsters use in recruitment include fake references or providing fake references for others to use. ChatGPT can be used in virtual/remote interviews to provide answers in real time. People can change their name in order to attempt to hide criminality that would otherwise appear on a DBS check. It all sounds really scary. But it isn't AI or digitisation that's scary – it's how it is used and the gaps organisations leave open for it to be abused.

There are benefits to AI and digital hiring. Use of AI for CV screening can help speed up the recruitment process, the use of gamification not only improves candidates perception of the work and the work environment, but also the recruiters can understand whether a candidate possesses the required job skills. We know software is being developed to detect tone of voice and eye movement during interviews indicating if someone is reading and is familiar with the content in the same way as advances to being able to identify grooming behaviour online is being developed.

The use of digital identity reduces the likelihood of people without right to work or the appropriate qualifications to get work, especially with children and adults at risk.

The single most important point for hirers to remember is that they are mitigating safeguarding risk. It cannot be obliterated. Thinking you have closed all the loopholes is the biggest risk of all! As Michael Bichard (Baron Richard) said in 2004:

" the harsh reality is that if a sufficiently devious person is determined to seek out opportunities to work their evil, no one can guarantee that they will be stopped. Our task is to make it as difficult as possible for them to succeed."

And it's not just about hiring. Not all perpetrators enter a workforce with the intention of committing fraud or abuse. Marcus Erooga identifies 3 types of child sex offenders which can be adapted to abuse and fraud in any setting:

• Preferential: those who are confident in their ability to evade, or not be subject to consequences or penalties, do not perceive obstacles, or are not easily deterred by them.

• Opportunistic: those who abuse because potential victims are available, potentially vulnerable, and the organisational setting either inadvertently facilitates, or fails to prevent, abusive activity.



MEETING MINUTES: SAFER HIRING 17th January 2024

• Situational: those whose propensity to abuse is previously unknown or unacknowledged, their offending is specific to the set of situational factors which potentiates their offending.

Erooga defines a protective system as one where someone who is thinking of abusing is aware that it is likely to be reported or detected and can be certain that if the abuse is disclosed not only will they be dismissed, but the matter will be reported to the police immediately. In such an institution, the risk-benefit analysis ought to lead them to the conclusion that whilst abuse may be possible, it is not in their interests to proceed. An aim of policy and practice, which includes organisational systems, must therefore be, to increase the risk and cost of detection to a potential perpetrator.

I think this shows how just one aspect of abuse cannot rely on a single mechanism of prevention. As part of the development of the Better Hiring Toolkit, a survey was undertaken to see what protective mechanisms employers relied on the most. The DBS check featured very highly. This is something that again Michael Bichard commented on in his report into the Soham Murders. He identified an 'over-reliance' on DBS checks. Whilst they obviously have their place, employers should never assume that a clear DBS check means they are employing someone who will not abuse and also that disclosed convictions/cautions and soft intelligence do not mean they are employing someone who will present a risk. Bichard's words from 2004 are as applicable today as they were then:

"There is a concern that many abusers do not have convictions and that no intelligence is held about them. Therefore, the selection and recruitment process, if properly conducted, is an important, indeed essential, safeguard."

How do we protect our clients, our staff and our assets? As employers, we need to be constantly horizon scanning, taking a 360 degree approach, assess and re-assess risk, not just at the recruitment, but during employment. Never relying on one method of mitigating risk but taking a multi layered approach – like Swiss Cheese!

The best way to describe this is included in the Better Hiring Toolkit – developing a safeguarding mindset.

A safeguarding mindset is the difference between compliance and curiosity. We know from many inquiries and reviews that a culture of compliance alone, meeting minimum standards and ticking the right boxes, does not keep people safe. For curious organisations who are actively curious about the information they do and don't have and explore further, when something does not seem right, they seek additional information to validate or challenge their observations. The Better Hiring Toolkit provides a rich wealth of resource about how organisations can set out their safeguarding expectations and demonstrate a safeguarding culture that goes beyond compliance and embraces curiosity. As part of this, the culture which promotes a freedom to speak up is crucial. Sharing conduct information and low level concerns is all part of this.



MEETING MINUTES: SAFER HIRING 17th January 2024

The issue of name changing, where applicants can hide criminality information by changing their name, is a good way of describing how BHI stimulates the conversation and provides resources to support employers. Although there is no evidence to suggest this is widespread, it can happen. BHI worked with a range of employers from a variety of sectors and government departments to develop simple guidance to help employers minimise the risk of applicants hiding criminality by using a different name. The work also underlined the fact there is no single solution/silver bullet and the importance of working together in this space cannot be over estimated.

At the other end of the spectrum, in the realms of public protection, is the issue of job scammers. BHI have supported JobsAware in the campaign to raise awareness of job scammers and the damage they do to unsuspecting job seekers. Although they may not fall within the legislative definition of being 'vulnerable', for people desperate for a job and for whom the cost of living crisis is biting hard, paying money for a check for a job that doesn't exist, and finding they have disclosed crucial personal identity information to a company who don't have a job to offer, can be utterly devastating to applicants.

An enduring theme in safeguarding is balance: the need to balance the need for vulnerable groups to be protected with the need to avoid unwarranted interreference by the state into private lives of individuals. This balance is still required as the safeguarding environment flexes and changes e.g. from physical to digital. In recruitment and employment the balance needs to be struck between getting good people into work quickly to benefit society, with the need to ensure we do not increase risk to the public and do all we can to reduce it.

Effective safeguarding is the same in the digital world as it is in the physical. It is less about place and environment and more about who those places and environments are likely to attract and what some of the inhabitants will exploit. The motivation to abuse systems for personal gain and gratification rarely changes, although the methods do. Adopting a safeguarding culture and organisational mindset at the point of hiring and beyond, where people feel safe to speak up and raise their concerns and where those concerns are critically considered is key in keeping the public safe.

3) Mike Haley, Cifas

- How much is hiring based on trust?
- How trustworthy are your hires?
- How do you know?
- Let me introduce you to Steven.

Steven worked in accounts in a small firm called Beetons, who sell agricultural products. At Beetons he was responsible for ensuring suppliers were paid and after a while he was trusted to set up accounts for new payees too. But Steven took advantage of his position and siphoned off £35,000 into his own account – diverting payments that were due to large suppliers. However,



MEETING MINUTES: SAFER HIRING 17th January 2024

he was found out and sacked. He was reported to the police, but they didn't prosecute as the amount wasn't much for a fraud and didn't reach their case acceptance criteria. Now Steven needs another job. He sees a similar job that he wants to apply but knows that his previous employer would provide an adverse reference. So, he does some Googling and finds a solution. He finds an online service that can provide him with a false reference and false career history, and what's more can field calls to verify anything he puts on his CV. He has found a Reference House. Steven applies for the job, and after interview and a test he is offered the job, his references are taken up and he passes the pre-employment vetting and joins the company.

Is Steven just a bad apple that slipped through the net? Or an indicator of a wider problem?

• How many people think that getting a job in this way is acceptable? To lie and present a falsified CV?

Fraud Behaviours Research

We polled 2000 people to find out the answer to that question. When asked how reasonable did they view CV fraud? 16% felt it was reasonable to falsify qualifications on their CVs.

When asked whether they, or anybody they know, had done this in the last 12 months? 21% admitted to either exaggerating their qualifications or knowing someone who had. Delving deeper, 4% said they had 'done it' themselves.

When asked what they would do if they found out a colleague had lied on their CV? Only 32% said that they would report it, 37% said they wouldn't, and 31% were 'unsure'!

The survey shows similar attitudes from people whether they are early or later in their careers. The survey showed that nearly a quarter of 16-24-year-olds and a quarter of 35-44-year-olds felt falsifying qualifications was a 'reasonable' thing to do. Interestingly The most likely age group to report a colleague if they found them to be committing this type of fraud was also 35-44-year-olds (41%). Surprisingly, perhaps the highest age group of individuals who said they wouldn't report a colleague for falsifying their CV qualifications was the 55-plus category (40%).

What is a Reference House?

So, 16% of potential applicants for a role think it's okay to falsify qualifications on a CV and 4% were prepared to admit it to a pollster. Amongst those there will be many who think it okay to do what Steven did and seek the services of a Reference House.

Reference Houses operate to provide false references and on occasion will also coach job seekers to give the impression that they have experience in the field they are looking to work. As well as advertising their services online, some will approach individuals in recreational settings. A Cifas member reported an instance of a job seeker being approached in a gym where for £600 they were promised a false CV and a crash course in KYC to enable them to work in financial services. As well as providing the false reference, for an additional fee they will also answer any phone calls in the name of the company the individual supposedly previously worked for.



MEETING MINUTES: SAFER HIRING 17th January 2024

And the way that some Reference Houses get around being able to provide false references is:

- Marketing themselves as offering documents for 'novelty' purposes; or
- Saying that they will provide duplicate documents or replacements of lost original references or qualifications.

And although there may be occasion when the purchaser may be for that reason – in the main they are providing fake documents to falsify a career history. Indeed, online Forums such as Reddit and the Student Room are full of posts where users are discussing the successes that they have had when using a false reference.

To counter the use of such services, Cifas holds bespoke Reference House Working Groups for our members so that they can share intelligence, and best practice for how they are identifying them. For example, best practice is to check whether the date the 'employing' company was incorporated at Companies House is before or after the candidate claims to have started working there.

So, what is Stephen up to now? Well, Stephen likes to gamble – it's his only vice really. But he has got himself in a little bit of money trouble and so he is just going to 'lend' himself a £1000 from the company to tide him over and he tells himself he will pay it back next month as he wants to keep this job.

Slide 4 – AI and the hiring

It seems therefore, that Stephen might be soon looking for yet another job... However, now when he looks for help to falsify his CV – he might be helped by AI. AI tools are being used to create CVs and aid interviews. And employers are starting to say that they will not consider hiring individuals who are suspected of using AI to write their CV or covering letter as they want these to be a true reflection of how the candidate can talk about themselves and their career history and not whether they can use a piece of software.

There have also been reports that in virtual interviews, candidates are able to use AI generated answers to questions they are asked, meaning that they are able to confidently give a comprehensive answer to each question asked without any hesitation, albeit not based on their real experience. In the past it was not unknown to hear of occasions when individuals would join an organisation and be identified as not the person who sat the interview, as they were paying somebody else to sit the interview for them.

Many interviews are now carried out remotely and the use of deep fake technology can alter the image so that the person sitting the interview and the person turning up on day one actually looks the same.



MEETING MINUTES: SAFER HIRING 17th January 2024

It's not always easy to spot whether a deep fake is being used, but there can be tell-tale signs if you are hiring remotely - if you have a degree of scepticism and look closely. Signs to look out for can be:

- a blurred face and hair.
- a change of skin tone or double facial features such as eyebrows.
- eyes which do not blink or unnaturally blink and facial movements that are not usual.
- un-natural light or changes in the background

• the voice does not naturally flow and background noise that is not consistent with the location.

Regrettably, I expect that deep fakes will become more and more convincing, but hopeful that new tools will arise that will be able to detect when AI is being used. Remote interviewing and on-boarding are opening up opportunities for job seekers and employers but create new problems. So, I want to bring you up to date with what happened to Stephen.

Unfortunately, it took a sinister twist. Because once in role, he was contacted by someone at the Reference House, and he was blackmailed. He was told that if he didn't divulge confidential customer data to them then they would tell his employer that he had used a false reference and false career history to gain employment. He started divulging information in order to keep his secret, providing sensitive commercial and personal information to the organised criminal gang that operated the Reference House – or who had gotten information from the Reference House.

Now this situation could have been avoided if Steven's original and prospective employer had been sharing information on employees dismissed for such conduct through the Insider Threat database. On behalf of our members, we operate a data exchange, the Cifas Insider Threat Database, which holds information on people exited for fraudulent or harmful conduct, such as accessing customer information. Steven would have been filed by his old employer and then searched by his prospective employer, with a match being identified and employment declined for not declaring their previous employer from whom they were exited.

So, what is the impact of such a case on business and in particular small business?

A report from HR Grapevine dated 24th November 23 demonstrates the impact of internal fraud:

A business founder who appeared on the show Secret Millionaire, was forced to sell his company, and lay off six employees, after a newly employed accounts assistant fraudulently stole £35,000 from the business. Aria Taheri, founder of Manchester-based Velo Systems, said that the fraudulent assistant accountant, Sarah Cunningham, "left a trail of destruction" that led him to selling his business at a loss and laying off six employees. Cunningham had been working for the company for less than a month when she started to transfer large sums of money from the company account into another account.



MEETING MINUTES: SAFER HIRING 17th January 2024

She had access to the firm's banking system but had to seek approval to make payments. As a result, she set up an account with a similar name to a supplier the company often works with, to try and disguise where the money was going. The people who handle the money in your company, arguably have the role that requires the most amount of trust.

Having adequate checks and balances in place to ensure that you are take on the right hires is crucial for business success. Such checks as:

- Identity Verification and Authentication including of remote applicants.
- Hiring staff being aware of the use of reference houses, diploma mills, and the ease of producing false documents; and
- Using external data sets to vet the candidates such as the Internal Threat Database.

I want to end with a quote from Stephen Bartlett, from Diary of a CEO – which is that 'every company, whether they realise it or not, is simply a recruitment company. Every CEO will be judged simply on their ability to hire the best individuals'

The question is why do so many therefore leave it to chance whether they will be the next company to employ Stephen or Sandra?

Open questions and discussion

Emma welcomed the new perspectives from the speakers.

James Morris MP - is there a distinction between the private and public sectors?

MH – no because verification and validation processes for jobs are the same. The Insider Threat database started with banks and spread from there until a LA did and found 14 applications in 9 months were from people with a fraudulent history. Thinks that there should be standard checks across all sectors. Fraudsters target HR jobs to recruit in their confederates, housing associations to get keys to houses etc.

Nesrine Ramadam – biomedical sector. Sometimes fraud happens using authentic documentation and recommendation such as academic papers. Fraudsters have targeted students and junior researchers who are offered more support and engagement to be successful in their academic field. No way to protect students who stand against it as the fraudsters can be in positions of power or authority. A culture of protection and awareness as well as awarding good behaviour is needed. How can we make sure that we can spot fraud committed through authentic routes.

MH – Academic fraud needs a good whistleblowing policy that protects people who come forward. If you lose trust in a department, it spreads through the whole organisation. In some sectors colleagues cannot believe that other colleagues could commit fraud e.g. Charities or the MoD. Need to get everyone engaged in the mission. In academia what is the mission that everyone is engaged with?



MEETING MINUTES: SAFER HIRING 17th January 2024

AMcD – there is work going on in the US around linking publications to people. No way to bind people to academic papers. It is about culture.

Sean Moran, Proclinical – where I live there are three different trusts. Each has different qualification requirements for the same job. It would help the Public Sector to have a set of standards for qualifications across all Trusts. Can we have a "passport" based on a common standard to stop opportunistic fraud?

DBS standards can delay hiring by up to three weeks.

KR - Working with healthcare to create an NHS staff passport. We are creating the hiring frameworks to build the toolkits for this. In the NHS, supply chain actors have to see documents face to face whereas the NHS itself does not. Some say digital is OK, some say manual is OK. We are working on a healthcare standard with those on the Advisory Board who are in healthcare. If you could hire people in a day, what a change that would make to waiting lists!

Scotland has a better system for dealing with DBS checking in the NHS. Last July we heard from NHS professionals about these frustrations.

Kezia Tobin, the 3 million – genuine applicants need to be protected. Immigration status for non-British citizens in the UK will be fully digital by end 2025. Biometric cards will not be in circulation anymore. To hire a non-British person an employer will then need to go through the new system. We are aware of real problems with the digital immigration system e.g. seeing other people's photographs or sometimes the system is down altogether. The Employer Checking Service is there as a back-up but many employers are not aware of this in the first place! Would like to propose that BHI has clear guidance for employers of non-British citizens, not always an indication of fraud. Invited the APPG to look into this seriously.

KR – November session was on this and took evidence from 100 employers. Next Thursday there is a live event with the Home Office to provide evidence. Please share evidence, we are aware of some of these problems.

Natalie McClean, Partners&– use an external referencing company. How much do they understand about the risks?

KR – this work will be the first guidance for screening companies as well as hirers. Not all screening companies are as engaged as others.

MH – Cifas has a number of working groups for FS screening companies. Tracey (Cifas), we do have a group to talk about onboarding issues. There is a Reference House working group. This does give an opportunity for members to share details of fraudulent businesses etc. Cifas can advise on which vetting companies people use and whether or not they use the Cifas database / attend meetings. Clfas can share information on threats and trends.

Matthew Rushton, RTS – Building on Mike's presentation, how do you stop Stephen from reoffending when back in the job market?



MEETING MINUTES: SAFER HIRING 17th January 2024

MH – not enough is being done about people who commit fraud, there needs to be a path back for offenders. Social Media encourages young people to get involved in fraud such as mule bank accounts.

David Crank, Association of Document Verification Providers – worried about fraud undermining the trust framework. The Trust Framework is vulnerable to the weakest link. Concerned about insider fraud or threats to staff who then commit fraud.

MH – Economic Crime and Corporate Transparency Act brings in a due diligence defence. Companies will have to conduct a risk analysis. Platforms like Meta are used by fraudsters to post jobs but have no incentive to correct this. Need to change the culture from the top.

Mark Sutcliffe – fake CVs are a problem amongst the 1.8m seafarers globally. Is there an international organisation to educate seafarers? How many individual cases happen per year and what is the cost to the economy?

Kelly Nelson, UK Defence – as tech becomes smarter and methods more sophisticated, how do you see employers' defence mechanisms having an impact on economically challenged candidates.

MH– no international arrangement around fraud. Do not think we know the number of CV frauds annually?

AMcD – with digital poverty, DSIT is doing a lot of work on inclusion such as creating different identities through the Post Office. Those with no passport or drivers licences need to be able to use other documents. No one answer to solve it for everyone.

KR – no data but looked at 100k job seekers and 1 in 4 had significant discrepancies. On Kelly's point, have run sessions on digital poverty. 1 in 5 job seekers cannot go through the digital route. DSIT is working on expanding the document set. Toolkit output will look at a one pager for MPs to help with constituents.

Non-Parliamentarians present

Lucy French, Amy Davis, Christy Houghton, Matthew Rushton, Lauren-Jane Edwards, Kiran Herkanaidu, Rachael Jones, Reed;

Keeley Robinson, Lemon-GS;

Michael Whittington, Certnco;

Shazia Imtiaz, APS Co;

Rajiv Ranjan Complygate;

David Shribbs;

Robert Stoner, Islington Council;



MEETING MINUTES: SAFER HIRING 17th January 2024

Home Office;

Kevin Feely, Ramsay Health;
Chris Price, Capgemini;
Jon Bains, Obsolete;
Shakeel Chohan, Open University;
Anton Background Check Advisory;
Del Millward, Appruvr;
Sara Al-sherif, Open Rights Group;
Christine Marie Morton, HSBC;
Laura Hanks and Lauretta Asak, Monzo;
Angus Sim;
Phillip Wood, Face phi;
Claire Beas;
Emma Shepherd, Letstalkdisability;
Beth Alberga EPM;
Katie Rountree, Hayley Kofoed, KPMG;
Emma Roche, Principality Building Society;
Adrian Field, oneiduk;
Grants Shipway, River-island;
Amelia Lyth, Foolproof;
Deedee Doke, Recruiter;
Penny Dunbabin, William Hebblethwaite and Deborah Awoyemi,
Carly Rochester, ME Passport;
Michael , Diligentchex;
Sean Moran, Proclinical;
Lauren O'Keeffe BCW-Global;
Ruth Rossiter, Linca;
Dylan Hibbert, 1993;



MEETING MINUTES: SAFER HIRING 17th January 2024

Natalie McClean, Partnersand; Kezia Tobin, the3million; Laura Turner, Surrey Choices; Jaya Patel, Islington; Kelly van Nelson, Serco-ap; Nesrine Ramadan, St Annes, Oxford University; Wayne Jones; Teresa Boughey; David Crack, CDD Services; Alison McDowell, Beruku Mike Haley and Tracey Gallagher Carpenter, Cifas