THIS TRANSCRIPT IS ISSUED ON THE UNDERSTANDING THAT IT IS TAKEN FROM A LIVE PROGRAMME AS IT WAS BROADCAST. THE NATURE OF LIVE BROADCASTING MEANS THAT NEITHER THE BBC NOR THE PARTICIPANTS IN THE PROGRAMME CAN GUARANTEE THE ACCURACY OF THE INFORMATION HERE.

MONEY BOX LIVE

Presenter: **VINCENT DUGGLEBY**

TRANSMISSION: **26TH NOVEMBER 2007** **3.00-3.30** **RADIO 4**

DUGGLEBY: Good afternoon. Events over the past week have shown just how vulnerable we are to misuse of personal information - not just names and addresses, but birth dates, bank accounts, credit records; in short, almost anything a criminal needs to steal our identity. It remains to be seen whether the loss of child benefit data by Her Majesty's Revenue & Customs has fallen or will fall into the wrong hands. So the key question for this Money Box Live is what can you do to safeguard your identity? What sort of password or PIN number should you select? How can you avoid hackers and phishers when you pay bills or buy goods online? And what's the point of shredding bits of paper at home when you're required to disclose so much sensitive information to banks, building societies and insurance companies, let alone the Inland Revenue, and then it's so easy to copy? Identity theft affects more than 100,000 people a year and the cost is getting on for £2 billion. Surely, you might think, more could be done to stop it? The National Consumer Council, for example, has been campaigning for one agency to help those whose identity has been stolen because, as Money Box has repeatedly warned, it is very difficult, stressful and time consuming to get your financial affairs back on track after the event. So in the next half hour, you can draw on the experience of my four guests. Ed Mayo is Chief Executive of the NCC and he's in our Grantham studio. Here in London, I have Sandra Quinn from APACS, the Association of Payment and Clearing Services; Jill Stevens from the credit reference agency Experian; and Roland Perry, who for the past 10 years has been a consultant to industry and government on computer security and internet policy. The Money Box Live number is 08700 100

444 and our first caller of many is Michael in Maidstone. Michael?

MICHAEL: Yes, good afternoon to you.

DUGGLEBY: Good afternoon.

MICHAEL: Thank you for calling me. I was on holiday in St. Petersburg earlier this year, St. Petersburg in Russia, where I was severely mugged. I had my wallet stolen with of course all my credit cards, store cards, my old driving licence with of course my full name and address and my signature on it. There was a lot of other personal information as well in my pocket… or in my wallet. I have been concerned since then as to whether my identity could get lifted from what they have got.

DUGGLEBY: Have you lost anything as a result of this that you know of?

MICHAEL: Not that I know of. I went straight back to my hotel, contacted my wife here in the UK who gave me the number of the card people. I spent 30… £40 on telephone calls that afternoon, Saturday afternoon, and all the cards were stopped …

DUGGLEBY: Okay, well let me just …

MICHAEL: …although they had been broken.

DUGGLEBY: Let me just stop you there because here is somebody - anticipating slight stress in your voice, I think - somebody who's clearly worried that this is not the end of the story, so let's start with you Jill and say what should he do?

STEVENS: If you are worried that your personal details, whether they be stolen in St. Petersburg or indeed in Margate, might be used to impersonate you in terms of getting credit in your name or other financial services, you need to check your credit report. It's quite easy to do and it's the only way you'll find out whether someone is actually applying for these things in your name at your address. We're

never going to be a step *ahead* of the fraudster, but if we know what we're looking for we can actually be perhaps enough steps behind to get something done before anything awful happens. For example if you see that somebody has applied for credit in your name or tried to open a bank account in your name, you can get in touch or we at Experian will help you get in touch with the lender concerned and we can perhaps get there before the loan goes out or before the credit card goes out.

DUGGLEBY: And that's a £2 fee for you or any of the other credit reference agencies?

STEVENS: It's £2. Or you can pay extra to have your credit report actually monitored so that we actually send you an alert if something happens and it changes on your credit report, if the information changes.

DUGGLEBY: Okay Sandra from APACS, it looks as though he did the right thing in terms of getting *very* quickly onto the phone.

QUINN: Absolutely, Michael did exactly the right thing he'll be pleased to know. We always say as soon as your cards are lost or stolen, phone up your bank and they'll do all they can. And the good news is he won't be liable for any of that fraud obviously.

DUGGLEBY: So Ed, is Michael right to still be worried then at this stage?

MAYO: Michael, you know I've been mugged and I really feel for you. And what you don't want is to be mugged all over again if your identity has been stolen, so it's right to take the measures that Jill and Sandra have suggested. I have to say that in the United States were you a US citizen, which by the sounds of it you're not, you actually probably have better protection and it's easier for you to get free credit references, you know free fraud alerts. So you know there's possibly a little bit we can do here in the UK following this fallout from this government blunder to make it easy for people who are in the situation that you are that are worried that this may come round again.

DUGGLEBY: Roland, your comment?

PERRY: Well I think that a lot of the problems these days come from organized crime and they're people looking to steal large amounts of data at once.

DUGGLEBY: Which might well be in Russia.

PERRY: Well they might well be based in Russia. But I don't necessarily think that, unfortunate though it is, going round stealing wallets one at a time is really their modus operandi.

DUGGLEBY: More operating on computers and stealing the information that way.

PERRY: Yes.

DUGGLEBY: They're pretty good at it, aren't they, some of the foreign criminal gangs?

PERRY: Well they can be very good at putting devices, various malware (we call it) on your computer to steal information off you, and then unfortunately it goes on sale on the internet and people can buy an identity.

DUGGLEBY: Picking up the point that Michael's made, an email from Cary in St. Alban's. He says the type of fraud that's being committed in connection with identity theft, such as relating to people who are applying for credit, "appears to prove the inadequacy of the systems that are in place at the moment. Why can't the banks and similar institutions do more to prevent this happening?" Are you doing enough, Sandra?

QUINN: Well we certainly do all the checks that we feel we need to do, but unfortunately there's no such thing as 100% security and that's why I think it is incumbent on all of us to look after as much of our personal detail as possible. I would stress that people shouldn't get worried about this unduly. The type of data

that may have been compromised by the HMRC loss last week isn't enough, for example, for anybody to get into our bank account, rummage around and move our money around, but it *is* unfortunately enough to take out new credit agreements in our name.

DUGGLEBY: Jill?

STEVENS: That's why it's very important to check your credit report to see whether or not somebody is applying for credit in your name. The thing to remember is that fraudsters are actually looking for all the pieces of a jigsaw, so why we were concerned about the child benefit information is that there is enough there for someone to have a good idea of what's missing. So in other words they can contact you and I'm afraid fraudsters are very clever and it's that nice young man on the telephone or that friendly email that comes from someone that it really almost seems like you know them, but they've got details about perhaps your children or where you shop or your pet's name - these sort of things that they can actually fool you into thinking that you can give them more information.

DUGGLEBY: So are children's birthdays now out as far as PIN numbers are concerned, do you think?

QUINN: Well I don't use them for my PINs, but I must admit that I did use my son's name and a combination of other numbers as a password to get into my bank account, which is a classic case of do as I say but not as I do.

PERRY: I'm not sure you should have said that on air.

QUINN: ***(Laughs)*** But I have changed that for exactly that reason, because there are a lot of people out there who try and use a PIN or a password that is intimate to them, that's close to them and is easy to remember.

DUGGLEBY: Okay, well we must move on because we've got too many callers stacking up to carry on on that subject. John, you're in Tadworth. You've got a question for us.

JOHN: Hello, yes. My credit card was compromised earlier this year. Fortunately I noticed within 48 hours, thanks to online access, and it was very quickly dealt with by my building society. And afterwards I decided to try registering with the CIFAS protective registration scheme. I signed up and chose a password and paid my fee. So a month or two later when I come to buy a car with a credit agreement, I warn the salesman there might be a delay in approving the application, but I was surprised a week later when the salesman actually asked me to write down my password on my credit application form. But I did do that and it went through. Then a couple of months later, with another credit card application, I had a phone call from the finance company asking me to give my chosen password for CIFAS and I thought hey, wait a moment. I asked them for a landline number I could call them back on. I recognized it was the right part of the country, so I phoned them back and gave them the password and that went through alright. So two out of two, it seems to be working, but I'm a bit uneasy about the way the system operates. I feel the password ought to be kept within CIFAS and I wonder if it ought to be changed after each use.

DUGGLEBY: John, you reflect the tenor of many of the people who have contacted us. They've been actually quite comfortable with what's happened and what the result of this last week has been is that they've got terribly nervous about things that actually haven't gone wrong and I think this is one of the things on this programme we're trying to address. So perhaps, Jill, you'd try and address this one again to credit application.

STEVENS: The CIFAS protective registration is a good system and it works. I do appreciate your worry there, John. I don't think it's supposed to involve the salesperson in the system and I think perhaps somebody didn't understand what they were doing there. Certainly if you are nervous about the fact that you might have revealed your password to somebody else, I think you can change it. I think you just have to get in touch with CIFAS and change it.

JOHN: Okay, I'll give that a go.

DUGGLEBY: Roland?

PERRY: And one of the things you did that was absolutely 100% correct was to phone CIFAS back. You should never give out any information …

JOHN: Well it wasn't CIFAS who called me in this case. It was the finance company for another credit application who had called me asking for the password, so again it was not CIFAS calling me.

DUGGLEBY: Check back though.

PERRY: Okay, but whoever it is who calls you wanting information from you, call them back because otherwise you don't know who they are. It could be anybody. It could be somebody trying to put together another of these bits of the jigsaw.

DUGGLEBY: Interestingly, John, we've had several emails on people asking for additional safeguards that they can introduce and several have mentioned CIFAS actually but one here has said they've been looking into a thumbprint protection scheme. Now I'm not going to name them because I know nothing about them, but I just wonder whether any of you consider these additional protections are of any merit. Ed from the NCC?

MAYO: Well I'm no security expert. I want to commend John though. I think you're a model citizen, model consumer and it's really good to hear that you were able to sort out that you know identity theft incident within 48 hours. You know I have to say whatever the protective measures are, from thumbprints to PINs, some of the people that we've talked to that have suffered from identity theft have had much longer, more drawn out experiences. It can go on for up to 2 years and sometimes really being passed from pillar to post before they get the information such as contacting CIFAS, as you have. So the world that we're moving into is a world that is more digital, more information is being exchanged. No doubt we'll get thumbprints alongside mother's maiden names.

DUGGLEBY: Roland Perry in the studio here - thumbprints, is that the future

or is it just another kind of possibility?

PERRY: Well people have been thinking about these sorts of issues for a very long time. I mean the sort of thing you might have is maybe even a smart card reader or something next to your computer that you'd put a card in that would prove that you were there. Maybe you'd have a fingerprint reader connected to your computer. I think the difficulty is connecting that fingerprint reader securely to the computer and then securely to the transaction at the other end is the difficult part. There are things called replay attacks where people can basically intercept your fingerprint going off to one trader and then they use it for another trader. And although these all sound rather unlikely scenarios, it's likely enough that it's put people off deploying this kind of thing at the moment, so I think it may be a few years before we see anything like that.

DUGGLEBY: Sandra, I'm a believer in random number generation. I use one of these little things which randomly generates a six figure number every thirty seconds. Is that the way to hit?

QUINN: Well we've started within the banking industry to roll out what we call two-factor authentication and that's essentially that type of data. You get a little gadget. They generally look a bit like a calculator.

DUGGLEBY: That's right, yeah.

QUINN: You put in your card, you enter your PIN. It generates up to a twelve digit number. You use that for that transaction only. And after that it has no use, so if anybody were to intercept that number it really would have no use to anybody afterwards.

DUGGLEBY: Now if you ally that with a credit card or a bank debit card or anything like that, as far as I can see it's reasonably foolproof, but is that so?

QUINN: I'm always rather chary of saying completely foolproof just because nothing ever is in this world.

DUGGLEBY: Never say never.

QUINN: But it is absolutely a new technology, it's working. Those banks that have already started using it have seen a noticeable change in their fraud losses as well.

DUGGLEBY: Is it going to be very expensive though for everybody to have one?

QUINN: Absolutely not. I think as we get comfortable with banking online, buying things online, it's being able to do things normally without putting ourselves out far too much.

DUGGLEBY: Okay, John in Newport, your call?

JOHN: Hello there, thank you. My point is, if everybody seems to be so worried about giving out their account number or everything, what happens if I want to buy goods by mail order? If I send a cheque I'm effectively sending them my name, my address, my sort code, my account number.

DUGGLEBY: And your signature.

JOHN: And my signature.

DUGGLEBY: Hmm, yes, that's an additional thing, isn't it?

JOHN: That's right.

DUGGLEBY: So who wants to tackle that one? I must say a cheque does seem to me to be… Well of course a lot of businesses won't take cheques any more of course. I don't think it's for security reasons. It's just probably because of cost of processing. But it is a point, you know, that a cheque contains an awful lot of information about you.

STEVENS: Just one point, John, is that to live in the world legally and comfortably, we do have to have a measure of trust and I think it's sad if we start thinking that every time we put a cheque in the post it's going to be intercepted. And I know that there are fears and I don't want people to panic. I think that Sandra can probably tell us how secure a cheque is. But I want to say that we do have to have a measure of trust, we do have to give our personal information to people in order to live legally. It's knowing who we're giving the information to and why we're giving it and just being a little bit careful and using commonsense.

DUGGLEBY: Sandra, the banks don't really check signatures any more on bits of paper, do they?

QUINN: No, absolutely not. What we do is check high value items. Over a certain level, there are more stringent checks being undertaken. But I think the point John has made about having your sort code and your account number on a cheque is absolutely valid. Lots of people always say to us, "Oh we're really concerned about giving that information out" until we say, "Well look, you've been giving and using cheques for a long time. You've never had these concerns." And, as Jill said, you just have to accept there's a tiny level of risk with practically everything we do every day. But with a sort code and account number actually all anybody can do is pay money into your account, not take it out.

DUGGLEBY: Okay, Chris has sent us an email from London and he's concerned about shared entrances. He says, "I have a shared hallway and I'm actually considering renting out my flat and a big concern for me is how easy is it for someone to take away all the sort of mail that comes in?" - and he cites credit card application forms and things like that. "I don't want this mail and I don't want to find if I rent my flat out that two or three months down the line, I suddenly find my identity being stolen." I guess that's a jolly real fear, isn't it Ed?

MAYO: Yes and in the work that we've done with identity theft victims, we've found that it's quite often the case that someone may move… You know one elderly lady who moved into a care home and you know her records were

taken by the tenants that had moved into her flat. You know when she died, actually her daughter had two years of dealing with the problems and the new credit that was taken out before you know that was resolved. So I think these are exactly the issues that will worry people where your home is open to use by others.

DUGGLEBY: I think one of the first things that obviously should be done is making sure that mail is diverted to the new address and for quite a period of time. Would you suggest that that's the number one priority, Lisa? Sorry Lisa … What am I talking about - Lisa? Jill?

STEVENS: What we say in the advice that we give to victims of fraud … And just to reiterate what Ed was saying, you may not suffer financially if you're a victim of identity fraud but it can be very, very distressing. People feel very vulnerable. It's not a personal crime. They really don't think of you as a person. You're a set of data, but it doesn't feel like that if you're the victim. So the important thing to remember is if you move home make sure the Post Office redirects all your mail. I do it for 18 months as a matter of course and if I think stuff is still going to the old address, I will actually elongate it so that it's 2 years. Make sure that if you see something coming via the redirection and it's still being addressed to your old address, write to that company or phone them up and make sure they've changed your address on their database. Also register with the mailing preference service. If you don't want junk mail, you don't have to have it in this country - so register with the DMA's mailing preference service.

DUGGLEBY: Roland, I suppose it's right to say that you can of course move a computer from one address to another and actually nothing changes at all because your electronic address is different?

PERRY: Well that's right. Pretty much your email address will move with you, so that's not an issue. But I agree, when you move house is a really good time to actually make sure you understand who your bankers are, who your credit cards are with, that you've got all the latest addresses and telephone numbers and contact details. And, yes, get the post redirected and do it in time (because it takes about a week) but also the Post Office will only do it for 2 years.

DUGGLEBY: Okay, we'll move on now to our next caller and it's Lesley in Penzance. Lesley?

LESLEY: Hello. My concern is that banks - well certainly my bank, which is one of the major banks - misuse the security checks that we as customers are supposed to go through, which confuses us customers and thereby aids the fraudsters. I can certainly give you one example. I can give you a few actually, but you've probably only got time for one. Should I go ahead?

DUGGLEBY: Well let's just take this general point of misusing information. What do you mean by misusing information? I mean if a bank calls you, they will obviously have to establish that they're talking to the person they say they talk to and I mean for example if somebody rings me up and my wife answers, they say they want to speak to me, so to that extent they are trying to get hold of the right person. The question really is how do they do this?

LESLEY: Right, well let me just …

DUGGLEBY: Let Sandra comment generally on the procedures used.

QUINN: I think this really plays back to what somebody else was saying earlier, Lesley, and what I would suggest is if you have any concern about any call that was made to you and you don't think you can verify adequately that they are the right person is put the phone down and phone back to either your bank or whoever on the number that you normally phone them on because that's the best way of checking that they are who they say they are.

DUGGLEBY: Right, Lesley?

LESLEY: Right, can I give you this example because it is relevant?

DUGGLEBY: Well briefly if you could.

LESLEY: Somebody from my bank rang me and immediately started with the question, “Am I speaking to Ms Lesley of Penzance?”

DUGGLEBY: Yes, correct, that’s fine.

LESLEY: I said yes. He then continued with questions asking me for my data of birth, my account number, at which I stopped him and asked him who he was and why he wanted to know.

DUGGLEBY: Well that’s fair enough.

STEVENS: I think you did the right thing there, Lesley.

LESLEY: He told me … he told me that until I answered his questions, he couldn’t tell me. Now, really alarmed, I refused to answer any more. So he gave me a number to confirm he was legitimate. I rang that number and was asked the same questions plus two digits of my security number.

DUGGLEBY: Alright, well let’s just stop there because obviously you know we don’t know what the exact facts are, but I do recognize what you’re saying and that is when a communication takes place, particularly if a bank wants to offer you some service, that they do ask certain amounts of information. I don’t quite see how they could do it any other way, but I do recognize the concern felt, Sandra.

QUINN: I think that’s absolutely right. Some customers do find this type of marketing difficult to manage and they feel that it’s putting an undue pressure on them. And I would also say that if you feel like that, just say that you’re not interested and if they’ve got something to market to you you’re not interested in talking to them. If it’s a *real* issue - if they’re concerned about whether your card has gone missing and you might be a victim of fraud - that’s a completely different issue. You’ll have numbers for that and you can always contact them back.

STEVENS: And don’t contact them back, Lesley, on the number they give you because on this occasion I’m sure it was somebody from your bank, but if it’s a

fraudster they are going to give you a number which will be part of the fraud ring, if you like. So use the number, as Sandra said, the number you know is the number you usually contact your bank on.

PERRY: Yes, I would say you know, Lesley, I think you've done exactly the right thing, but you were just put into a very, very difficult place. And I think that we need to recognize that as individuals we can take responsibility and we need to take responsibility, but so do these big organizations that handle our data. It sounds to me like your bank was being stupid in what it did. That's what we've had with the government blunder as well. We're all vulnerable to identity theft, however much we shred our papers or take care of our PINs, if we're not sure that the big agencies that handle our data aren't managing that data well and not releasing it in silly ways. It's got to be on both feet.

DUGGLEBY: Right, we must on. Lisa in London, your call now?

LISA: Hello. I'm concerned about the data that government departments have and possible laxity they show on certain of their procedures because I recently started to claim the state pension and I noticed last week that my pension comes into my bank account with my full national insurance number printed as a reference on my bank statement together with my name and address. Now I phoned the pensions department and asked them to remove this number as a reference or to use only part of it and they told me that all state pensions go out monthly with this national insurance number quoted and that I should ask my bank to do something about it. And when I asked my bank, they said they couldn't alter the reference number …

DUGGLEBY: Can I stop you there …

LISA: …of income and credit.

DUGGLEBY: …because I want to bring in Roland in here because one of the things that I think has arisen from the HMRC case is the inability to screen out information. Now are they being correct when they say that actually this information

is quite easy to screen out and they're saying that you can't do it because that puzzles me?

PERRY: Well there's all sorts of reasons why you can use the national insurance number as, if you like, a nickname for somebody. In fact in this case it's one of the very few reasons that's legitimate - lots of people misuse the information. I would say that actually I don't regard your national insurance number as a secret in that sense because so many people do have the number. It's known to huge numbers of government agencies, it's known to every employer that you've worked for. It's known to the payroll organizations that your employer might use. So I wouldn't be too worried about just the national insurance number.

DUGGLEBY: Okay, Roland, well you're a computer expert. What is the one bit of information that might be included on any piece of paper that you've got from a government agency which would worry you if it was on there, or what would you take off if you could? I mean is it date of birth? Is it, you know, wife's name or children's reference numbers or what?

PERRY: Well what it shouldn't have on there - and I don't believe I've ever seen it on there - is any one of these so-called shared secrets, so your favourite colour, a password or anything like that. If it's real information from the real world like, you know, your real name or …

DUGGLEBY: Factual information?

PERRY: …factual information - if you're married and it's your maiden name - that is information, that's factual information. Your date of birth is factual information. People will find that out anyway.

DUGGLEBY: So it's something which nobody would know unless they'd actually personally either spoken to you or seen it written down, right Sandra?

QUINN: Absolutely, I completely echo what Roland says. Factual information - your date of birth, your name, your address, even your children's names

- people can find that out. That in itself is not top secret information. It's available somewhere. What *isn't* available, unless you share it with people, are the private things - the PINs you use, the passwords you use - and that's why we stress it's a good idea to keep them as secret as possible.

DUGGLEBY: Your first motorcar or something or where you first went on holiday - that sort of thing which apparently only you are supposed to know. I wish I could remember. Right, final call from William I think it is. William?

WILLIAM: Yes, hello Vincent.

DUGGLEBY: Hello. My preoccupation is exactly the same as that of the lady who spoke to you before. Because I receive the £200 fuel allowance for Christmas - I'm over 60 - it's come up on my bank statement identifying my national insurance number. And also the statement has come in an envelope which not only shows the name of the bank, headed "private and confidential". On the rear of the envelope, it shows the address from which the bank statements are sent.

DUGGLEBY: In other words, you don't think the means of communicating it to you - i.e. through the post - is being very securely handled?

WILLIAM: Also, they just have to open it and immediately they've got my name, my address, my bank account number and my national insurance number.

DUGGLEBY: Okay, this theme, William, runs through a lot of the calls. People are very, very frightened about this information and I think what we've tried to do on this programme is say that some of this information is not so sensitive as perhaps you think it is. So a quick comment from the panel.

STEVENS: I just want to say we've been using the post, we've been using cheques. We have to have some sort of a level of trust in life and I really think that we mustn't get panicked about this. We mustn't assume that everything's going to be vulnerable. So let's just be commonsensical about it.

DUGGLEBY: Ed Mayo?

MAYO: Well I agree with that. In some ways it's like you know a kind of rusty central heating system: you don't want to think about it, but if it goes wrong then it can be quite disastrous. And that's why I think one of the things we're campaigning for at the National Consumer Council is this one stop shop for people who do suffer it, because it really is so traumatic for people to suffer identity theft. And I think it's quite right for William and other callers today to really worry about the data that's out there.

DUGGLEBY: Roland?

PERRY: Yes and I think the banks and other financial institutions have made great strides in recent years in anonymising envelopes that they send you. It doesn't say from x, y, z bank on the back any more.

DUGGLEBY: And Sandra?

QUINN: I would hark back to the comment that Roland made earlier: organized gangs aren't just emptying one or two envelopes.

DUGGLEBY: Okay. I'll leave you with this thought from Wendy in Oxford and she says, "Given that we are constantly told by the Government to shred all our sensitive information in order to avoid identity fraud, do you think that under the circumstances I should get tax relief on the cost of my newly purchased shredder?" That's all the calls we have time for. My thanks to Ed Mayo from the NCC; Sandra Quinn from APACS, the Association of Payment and Clearing Services; and Jill Stevens from the credit reference agency Experian; and also computer expert Roland Perry. If you'd like more information on any of the points we've raised in the programme, then the number to call is 08700 100 400. We have our website, bbc.co.uk/moneybox, where there are links to other sites and details of how to get hold of the podcast. Don't forget to join Paul Lewis on Money Box at noon on Saturday, and for the next few weeks Paul will also be taking your calls on Money Box Live.