

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: PAUL LEWIS

TRANSMISSION: 9th MARCH 2011 3.00-3.30 RADIO 4

LEWIS: Hello. Fraud is alive and well and living among us, and today Money Box Live is taking your calls on card, bank and cheque fraud as well as ID theft. Although this kind of fraud is said to be in decline, last year crooks got hold of more than a third of a billion pounds of our money illegally. Stolen cards, counterfeit cards, ID theft, pretending to be other people on the phone - it all adds up to a big criminal enterprise. But what can we do if we're the victims of one of these crimes? How sympathetic are the banks or card companies? How long will they take to sort it all out? Who bears the cost of the fraud? And there's even confusion over who we report these crimes to. Is it the police or our bank? Better of course if the crime is never committed or if you prevent it happening to you, but how can we protect ourselves against them? The banks are all trying to sell us insurance, but is that really the answer? Or does it just take normal vigilance like closing all our windows when we leave the house? Whatever your fraud question, you can call Money Box Live now: 03700 100 444. With me today to answer your questions on fraud are Jemma Smith representing the Financial Fraud Action UK; Detective Chief Inspector Paul Barnard, who heads the Dedicated Cheque and Plastic Crime Unit - also known as DCPCU; and Neil Munroe, External Affairs Director of the credit reference agency Equifax, and also Chair of the Identity Fraud Communications Awareness Group. Our first question is from Victoria who's calling from Essex. Victoria, your question?

VICTORIA: Oh hello. My card was fraudulently cloned when I was on holiday in Turkey. When I came home, I hadn't actually realised because the transactions going

through on my card were quite small but frequent. When I did actually realise, I reported it to my credit card company and they originally were very sympathetic. They seemed to change their mind and said that they weren't accepting those transactions as fraudulent. They were my responsibility, I should have reported it to them sooner, and I'm now liable to pay for it.

LEWIS: Just tell me again, Victoria, how long you left it before you reported it?

VICTORIA: It was actually quite a while. The fraudulent activity started in September 09 and, unfortunately, I didn't recognise that until the end of November last year.

LEWIS: Oh I see.

VICTORIA: So it's gone on for over a year.

LEWIS: So it was more than a year. And that was just because, like I'm sorry to say many of us, you didn't check your credit card statements quite as carefully as you might have done?

VICTORIA: No. I literally scanned them, checked out how much I had to pay every month and paid it. The amounts going through were so small, I just didn't recognise it. I didn't even give it any thought.

LEWIS: Sure. But obviously now you have discovered it, you'd like your money back. Jemma, Jemma Smith?

SMITH: And Victoria, was that on your credit card, sorry, or your debit card?

VICTORIA: It was a credit card, Mastercard.

SMITH: Well I am a bit surprised that the credit card company has given you that

response in terms of a time delay because there aren't any time limits on a fraud claim on a credit card, unlike a debit card where you've got 13 months. So all I could suggest is that if you go back to the credit card company and explain that you know that there are no time limits. See what they say. If they still turn you down, you can follow their formal complaints procedure. If that still doesn't get you your money back, then you can take it to the Ombudsman who'll take a look at it in an impartial way.

VICTORIA: I think I might do that. They started saying originally as well that I didn't have to pay any of the money on my credit card back until the fraud situation was sorted out. And when I didn't make my monthly payments, like I had been normally, they started getting collection companies involved on my account. And I've actually now had to pass it to a debt management company because the charges and administration fees they were adding onto my account every month actually pushed my card over its limit and I can't afford the repayments on it now anyway.

LEWIS: It sounds to me as if you've got a pretty serious complaint to make there, Victoria. How it will be resolved will be hard to predict, but Jemma?

SMITH: Well certainly I think you know time is of the essence now and I think that it's really important that you take down a note of all the conversations that you can remember that you've had with them, collect all that information together of any money you've paid out, so that you've got that all to hand.

LEWIS: Neil Munroe?

MUNROE: Well what I would suggest is that you actually also - if it has impacted your credit rating, which it might have done - get a copy of your credit file. And get a statement on there (which you're allowed to do) explaining the circumstances, so that if you are trying to get credit elsewhere, it doesn't look one-sided. You know you have your say on there about what's happened. That will be looked at by future lenders. So just to help you along the way while you get it sorted out, that you don't get hindered elsewhere.

LEWIS: And given the complexity of this - if it does turn out that Victoria gets all her money back, will she be able to clear her credit record because she has failed to pay a bill?

MUNROE: If it's not her fault and the lender's prepared to say that - then yes it will, we would clear the file.

LEWIS: It will be cleared.

MUNROE: We can get the lender to do that. And we as credit reference agencies can raise disputes with lenders on that basis. So once it's sorted out, if they don't (and they should do) correct it automatically, then we can certainly pick that up on your behalf and put it back to where it should be.

LEWIS: And the proof would be a letter from the credit card company or something like that, but that's all got to be sorted out first?

MUNROE: I think it would have to be, yes.

LEWIS: And the credit reference agencies, Victoria, are Equifax, Experian and Callcredit, and you can find them on the internet fairly easily. But do be careful because there are other companies with very similar names that want to get you to click on their site and you might be subject to yet another fraud. And your credit record will cost you £2 if you find the right spot on the website. I do encourage you to do all that because you've obviously got into quite a mess, a lot of difficulties because of this, and it really is important to get it cleared up. And I think most of us seem to feel it probably wasn't entirely your fault at all, so please take those steps quickly. Is that helpful?

VICTORIA: I will do. Yeah, that's brilliant.

LEWIS: Thank you very much, Victoria.

VICTORIA: Thank you.

LEWIS: There was a bit of detail there. I'll just remind you at this stage everybody listening that the transcript of this programme will be on our website: bbc.co.uk/moneybox. And right away, almost after the programme, you can hear the programme again through iPlayer. Same place: bbc.co.uk/moneybox. Russell now is in Addingham. Russell, your question?

RUSSELL: Good afternoon, Paul. After using the internet banking for many years, it was just this morning for the first time I logged onto my internet banking site as normal and it became apparent fairly quickly that there was something awry. As well as the usual two security questions I was being asked, there was a third one which was asking me to disclose my full PIN number. I then contacted HSBC - that's the bank I'm with - by phone, and they confirmed that I was on a different website and that under no circumstances should I give any details. My question was if I hadn't have been so vigilant and in a busy day had actually gone ahead and disclosed my number, my account had then been hacked into and funds had then been withdrawn, what would my position be?

LEWIS: Well it's a strange tale, Russell, really, isn't it? You say you logged on as usual to your HSBC website ...

RUSSELL: Correct.

LEWIS: ... and got another website.

RUSSELL: Yes.

LEWIS: That is very odd. Jemma Smith?

SMITH: Yeah, Russell, good on you for spotting that because I think nowadays these scam websites that do crop up, that are usually actually on the back of a phishing

email which I think all of us have received into our email inbox that seem to come from our bank, asking you to click on a link and it takes you to a dud website. Clearly that hasn't happened to you, but these websites a few years ago didn't look anything like the genuine website. Nowadays they are so close to the real thing, you'd have ...

RUSSELL: *(over)* It was identical.

SMITH: Yeah, you'd have hard trouble spotting it. So I mean just to reassure you, in that situation if you had have disclosed your details, you wouldn't expect to be liable for any losses had you done so. You know and that actually is across all types of payment fraud - your current account, your cards. If you're the innocent victim, you should get your money back.

LEWIS: Yes, well done for spotting it, Russell. And I think it's worth saying to everybody that no bank certainly that I know of will ever ask you for your full PIN. They will ask you for digit 1 and digit 7 or whatever.

RUSSELL: *(over)* That's exactly what they said and that's what alerted me.

LEWIS: That's what alerted you. So it's always worth being vigilant. So well done, Russell. And yes I'll just bring in Paul Barnard here, Inspector Paul Barnard.

BARNARD: Russell, the National Fraud Intelligence Bureau just around a week ago - and you can go online to look at their website - launched an exercise against phishing email attacks such as this because they're trying to sort of scope the scale of the problem. So I'd encourage you to have a look at that. And also the warning to everyone again is you know your banks do not call you asking for your personal details, your card details or your PIN number either by email or by telephone. Well spotted. Was it the usual link you always use?

RUSSELL: Yes. And if you don't mind, could I just pass onto the listeners what they advised me if you don't mind?

LEWIS: *(over)* Do, yes please do.

RUSSELL: Rather than going to the website via, well in my case Google or a search engine, they suggest that you should always type in the exact bank email address - website address, I'm sorry - rather than going through a search engine where you may be redirected.

LEWIS: Yes, I think that's perhaps what's puzzling us. Though I must say I did look on Google for HSBC and all the sites that came up were HSBC.com and seemed to be genuine. But it can easily be done - so, yes, type in an address you know or indeed store it on your favourites. And was there another question you had, Russell?

RUSSELL: Yes. Your first caller may have answered it, but a year or so ago a business colleague of mine had his credit card cloned and he told me that credit card companies will stand any loss if the card is cloned; whereas banks through their debit cards actually won't. So I changed my sort of behaviour where all my purchases now are done on my credit card, which is settled at the end of the month, rather than using my debit card which I only now use in the ATMs.

LEWIS: Yes, it also gives you more protection if something goes wrong with what you've bought. And just before I ask Jemma to comment on this, we've had an email on exactly the same lines from John who says, 'I prefer using a debit card rather than a credit card' because he doesn't want to get into debt. Reasonable enough. 'But someone told me credit cards were safer than debit cards' - exactly the point that Russell was making. Are they?

SMITH: No, you do get the same level of protection. No matter how the fraud has happened, you should get your money back if you're the innocent victim. However there are some slight differences in that with a debit card, you should expect immediate refund from your bank; and also you have got a timescale with a debit card to make the claim, which is 13 months. But I think maybe the background issue to people saying just sort of generally that credit cards are safer is that of course a credit card isn't connected to your current account, so the money isn't yours in the first

place. So perhaps people feel more comfortable using a credit card in higher risk situations.

LEWIS: You can still be asked for it back though, can't you? I mean we had that with Victoria earlier and I've also had an email now from Joel who says, 'My credit card was used fraudulently. The company was made aware of it and the total spent was refunded. But I still got sent a bill asking for the minimum payment. Because it was fraud, I didn't pay it. Then I got penalties for missing the payment. Again these were refunded. Then I got charged interest on the penalties, which again I didn't feel I should pay and I ignored it and it was again refunded'. So all the money was given back to him. But now he says his credit rating's affected because he got turned down for a new card. So although you say you get your money back, Joel obviously had a bit of a fight and you know Victoria earlier had a great fight.

SMITH: Yeah. But I would say that by and large the vast majority of people who are victims of fraud - and I think you'd be hard pressed to find anyone in the country who hasn't been a victim of card fraud at some point along the way - they do by and large get their money back without any quibble.

LEWIS: By and large. It's just the ones that don't that email us, I suppose.

SMITH: Yes. But I mean the most important thing is if you don't get the answer that you expect to get is that you don't ignore it and do something about it.

LEWIS: And there is an occasion though, isn't there, when you have to find the first £50?

SMITH: Well that is in the legislation when it comes to credit cards, but actually I've never heard in all the years of dealing with fraud claims of anyone having that imposed. I think it's really there to encourage us all to report the fraud as quickly as you can to your card company.

LEWIS: That's the first £50 if it's taken out between the card being lost and you reporting it?

SMITH: You reporting it, yuh.

LEWIS: Yeah, okay. And what about the burden of proof because that was something that changed recently too? In the past ... You may not agree with this, but our impression tended to be that the banks would always assume it was your fault and then eventually pay up if they thought it wasn't. Now they're supposed to refund the money and then do the research. Is that right?

SMITH: Yeah I'm not going to agree with you, Paul. I am going to say that the burden of proof has always been actually with the bank and that hasn't changed. But now it's actually in legislation, which means that you as a customer know that it's down to your card company to prove any negligence on your part.

LEWIS: Okay, thanks very much for that. Thanks to John for his email and thanks to Russell in Addingham for his question. And we'll move on now to Pamela who's somewhere in Greater London. Pamela, your question?

PAMELA: Yes, I was at a cash point just a little before Christmas. I wasn't using my usual one, which is HSBC. I was using NatWest because they have a reciprocal arrangement. I'd put my card in, I'd pressed all the right keys. I was trying to just sort of have a quick think how much money did I want to draw and a voice behind me said, "I hope it's working". There was another man on my other side with a piece of paper which he kept on pushing in front of me, in front of the screen and the keys. Suddenly one of them had gone. The other man kept on saying, "Give me fifty pence" and I said, "No, go away", and I realised that there was no money coming out to me; that whatever I was going to ask for had been taken. So I went across the road to the HSBC, which is my bank, and said "Can you tell me how much money has been taken out of my account or if any has?" Well it had.

LEWIS: That's a very distressing story, Pamela. So in fact they took the money

before you'd even got your hands on it from a cash machine by distracting you really?

PAMELA: Yes.

LEWIS: Let me ask Chief Inspector Paul Barnard about that. Is that a common kind of crime? A very distressing one clearly.

BARNARD: Yeah, Pamela, it's very distressing. Have you reported this to the police?

PAMELA: I reported it. I went straight back to ... After I'd been to my bank and they'd found out how much money they'd taken, I went back to the block of flats where I live, which is only about ten minutes away. I reported it to the warden who is an ex-policeman, and he told me which police station to report it to and I did it straightaway.

BARNARD: Yeah unfortunately, it's not uncommon to ...

PAMELA: *(over)* No, I know.

BARNARD: ...to have a distraction theft like this. There are several things that can happen at cash machines. One is a distraction theft that you've reported. And there is also a slight rise as well in what's called cash trapping where the cash slot on the machine is actually blocked with a piece of plastic, with sticky stuff on the back of it so your cash doesn't actually get dispensed. But this one in particular is quite distressing - that they were actually able to distract you in that way and then take your money.

LEWIS: And, Pamela, did you get your money back?

PAMELA: Well the HSBC got in touch with NatWest that afternoon and said that NatWest would refund the money, which they did. But a couple of weeks later, they

took it back again.

LEWIS: And you still haven't got it back?

PAMELA: No.

LEWIS: And why did they take it back? Do you know?

PAMELA: I don't know. They haven't been in touch with me. So when I eventually told my son what had happened, because I didn't want to distress him or give him my problem, he wrote to the NatWest but hasn't had a reply.

LEWIS: Jemma Smith?

SMITH: First off, Pamela, I'm so sorry. What a time, what a dreadful thing to happen. But I think that again in this situation, I would suggest that actually, unfortunately, making a fuss is exactly the thing to do, and going back to your bank and asking them to explain why they were prepared to give you the money but then changed their mind would be the thing that you should do.

PAMELA: Yes.

LEWIS: And just Pamela, so I'm clear, I may have missed this. Your bank is NatWest. You were using an HSBC machine.

PAMELA: Well my bank was HSBC. I have now been changed ... my family has moved me over to NatWest, so I'm now between the two.

LEWIS: I see. Which account did it come out of - a NatWest account?

PAMELA: No, HSBC.

LEWIS: It came out of an HSBC account.

PAMELA: On a NatWest ... They have a reciprocal arrangement with ... You can use an HSBC card in NatWest.

LEWIS: Sure, yes. And how much was it? May I ask you?

PAMELA: 200.

LEWIS: £200.

PAMELA: Yeah.

LEWIS: Well I must say my advice would be to go and complain in writing to the bank and possibly send them a copy of what we've been talking about today. Jemma, a final bit of advice for Pamela who's obviously had a very distressing time.

SMITH: Yuh, I think you know say that you want to follow their formal complaints procedure because that means that it will get looked at. And, again, if that doesn't get you the answer that you need to get at the end of that process, you can refer that to the Ombudsman.

LEWIS: And the Ombudsman upholds more than half the complaints that are sent. Paul Barnard?

BARNARD: It goes without saying there's clear evidence of criminality here. You should also include the crime number with that report to the bank as well.

PAMELA: Yes, I've got all that sort of very carefully down and I've kept it all.

LEWIS: Good. Well it seems to everyone here you have a very strong case, apart from our personal sympathy for you Pamela. So we do encourage you to pursue it

because £200 is a lot of money, especially when ...

PAMELA: Yes, I was going to ask for £50, you see

LEWIS: Yes, so they pressed the buttons as well. Pamela, thank you very much for your call and do pursue it because we all think you should get your money back. And I'm sure if NatWest or HSBC are listening, they're probably rushing off to find your case very soon. Thanks very much for your call. And we'll move onto John now who's in North Somerset.

JOHN: Hello.

LEWIS: John, your question?

JOHN: Yes, it really concerns fraud in the purchase of a motor vehicle on a very well-known website specialising in the buying and selling of cars. And very quickly, the fraud started because an embedded email appeared in the advert and enticed us to click on this rather than on the email button provided by the website host.

LEWIS: So you were taken off the website you thought you were on and put onto another one?

JOHN: Exactly.

LEWIS: And that resulted in money being lost, I imagine?

JOHN: Yes, £3,200 ...

LEWIS: Good grief.

JOHN: ... through what I believe is called an escrow scam.

LEWIS: Right.

JOHN: So this is where money is held, ostensibly by the website operator, and it's by a protection scheme which actually doesn't exist at all - and until you've seen the car, you're happy with the car, at which point you take ownership of the car and the money is then released to the seller.

LEWIS: But all of that presumably was simply lies to get hold of your money and then they've gone off with it?

JOHN: Exactly.

LEWIS: Yes. So what's your question, John? It's very unfortunate obviously, but what's your question?

JOHN: Well the question is what responsibility do the website operators have in these circumstances to attempt to reclaim the money?

LEWIS: Right. It's very hard ... People here are looking a little bit blank at this point, I have to confess. (*laughter*) Paul Barnard, this is clearly a crime. What can be done about it?

BARNARD: It's clearly a crime. It sounds like the website has been hacked into, and this is not uncommon that people are taken off site to a centre like this. You know there is opportunity to report it, as I say. It's clearly very difficult though to track down always where this type of crime has originated from. But, as I said earlier on, the National Fraud Intelligence Bureau are taking a huge interest in phishing type emails. You know there is an opportunity to report it to local police. But this is unfortunately about the use of technology, and I think the best form of any defence here is protection for yourself.

LEWIS: It's difficult though, isn't it? If you're on a website you trust - and I presume

this was such a website, John, that you're familiar with ...

JOHN: Yes.

LEWIS: ... and there's a button on it. That website, it seems to me - and I'm sure you agree, John - it should have some responsibility for the people who put adverts on its website.

JOHN: Well I think this is the point really. And it's how far they go in offering that protection. And in the first instance there is a link - along with a whole bunch of other links, so not particularly highlighted - that takes you to advice about fraud, but only the sort of proactive warning comes up when you click on the website's own email service to put you in contact with the seller.

LEWIS: Let me ask Neil Munroe for a comment.

MUNROE: Well very quickly, John, I think you should probably try and trade on their reputation and go to them and talk to them about this because obviously they're not going to be keen on too much publicity around this sort of activity and they should have some sort of obligation I think to check content of sites and links that are going on there just out of people wanting to use it and trusting it. So try that. Have a look at their terms and conditions as well because they should be published on the site. Go into those and see what they say.

LEWIS: And see the complaints procedure because all respectable websites, which John assures us this was, have complaints procedures.

MUNROE: Absolutely.

LEWIS: And follow that and follow it to the end because it's a lot of money to lose in a moment like that.

MUNROE: It is indeed. I'm sorry for you.

LEWIS: Thank you very much for your call and I'm sorry we can't give you an answer, but I think pursuing it with the website is probably a thing to do. We've had a message from Greg who says, 'When I purchase online, the company taking the card goes to VeriSign' - I'm sure we're all familiar with that extra layer of protection for authenticating the payments, But Greg, obviously following Money Box advice, has read the terms and conditions carefully and it says in the terms and conditions 'if there's any fraud, I - i.e. Greg - will be held responsible'. So is he signing away his protection by going through VeriSign?

SMITH: No, he's not.

MUNROE: No.

LEWIS: No? A lot of shaking of heads, Greg. So we're all assuring you that's not the case, though you're obviously worried it's in the terms and conditions, which maybe we should have a look at. Anyway, thank you for your message. And we're going to Rachid now in Birmingham. If you could be brief, Raqeed, because we're coming close to the end of our time.

RAQEED: Yeah, hiya. Basically what happened was about 8 months ago my credit card went missing and someone managed to take out £1800 on my credit card. I was told by my bank to report it to the police, which I did. The bank then turned round and said to me that as my wife knew the PIN number to it, I hadn't secured my PIN number, well I didn't keep my PIN number in a secure place, and so I'm liable to the £1800. I did try and contest it, but it was getting nowhere, so I decided just to pay the money off. My question is: is there anything that I can actually do about it to get my money back, and can they do that to me and say that it's not their responsibility?

LEWIS: Right. And was there any evidence really that you'd been careless with your PIN?

RAQEED: No. I hadn't written my PIN number down anywhere. The only thing I can think of, because my credit card was stolen from work, was that someone has possibly seen me, was looking over my shoulder or something when I was putting the PIN number into the machine.

LEWIS: Sure, 'shoulder surfing' as it's called. Paul Barnard, that's fairly common.

BARNARD: Yeah, shoulder surfing is very common, particularly at ATM machines. Is that where you used it, Rafeed, in an ATM machine?

RAQEED: Yeah, I used it at a ATM machine, but I also used it in the store that I worked at at that point. So I'm not sure where it was that it actually happened.

BARNARD: Yeah it's very difficult to say, isn't it? But you should always shield your PIN, as you know, because some ATM machines we do know can have PIN hole cameras fitted above them by criminals. They try and record the PIN number you're putting in. So I would encourage you to cover it not just with your hand; but if you have a wallet with you, also cover it with the wallet as well.

LEWIS: Yes because your force arrested some people, in fact got them convicted the other day of using those kind of machines on rail ticket dispensers, didn't they?

BARNARD: Well yeah, that was the British Transport Police. But certainly our unit is responsible for the investigation of skimming machines, etcetera.

LEWIS: Jemma, let me ask you. Having somebody using your PIN is not evidence that you've been careless, is it?

SMITH: No it's not, but I think that it's a very tricky one because you've got a situation where probably there's something in your terms and conditions about not sharing your PIN with anybody first off. And then secondly you've got the legislation which is obviously about taking care of your PIN. Now you know is giving your PIN

to your wife or a friend or family actually taking best care of your PIN? That I think is not straightforward.

LEWIS: But you see despite all the protection that we're supposed to have, this does seem a bit to me like a bank finding a little loophole and saying oh well, Raqeed, you told your wife what your PIN was ...

RAQEED: Yeah.

LEWIS: ... and so we're not going to give you the money back. Whereas the assurance we've had for the last half hour is you will always get your money back.

SMITH: Well you know it will always be looked at on a case by case basis. Again you know the only thing that Raqeed could do is to go back to his card company and plead his case, follow the formal complaints procedure and take it to the Ombudsman.

LEWIS: But the burden of proof is that they have to prove you've been fraudulent, not that you have to prove you've not been fraudulent?

SMITH: That's absolutely true.

LEWIS: Right. So I think follow the complaints procedure ...

RAQEED: *(over)* So I can still deal with now, can I? I can still go back to them?

LEWIS: I'm sure you can, Raqeed. We have to go because we're out of time. But yes, follow the complaints procedure and ultimately go to the Ombudsman and see what happens. But that is all we have time for. We've had lots of calls. My thanks to Jemma Smith from Financial Fraud Action UK; Detective Chief Inspector Paul Barnard of the Dedicated Cheque and Plastic Crime Unit; and Neil Munroe from Equifax. Thanks to all of you for your calls. Sorry that we didn't get through them all. There's more about fraud on our website: bbc.co.uk/moneybox. Now I've just got a

moment to say three weeks today, on March 30th, we will be doing Money Box Live live in public, in Plymouth, at the Drake Circus Shopping Centre. There'll be people there all day to answer financial questions as part of a BBC money advice road show. So if you want advice or just to watch us all in action, that's Plymouth on March 30th. I'm back at noon on Saturday with Money Box.