Banking Protocol

Debra Linge - Lloyds Banking Group

UK FINANCE

BANKING PROTOCOL

- The Banking Protocol was developed in response to a significant increase in vulnerable adults becoming a victim of a scam or fraud.

- The Banking Protocol is a partnership between UK financial institutions, law enforcement agencies and victim support and was rolled out in a phased approach, starting with the Metropolitan Police and London branches in October 2016 and is now live across all 43 police forces in the UK.

- The key aims of this partnership are:
    - *To identify individuals who are tricked into going into their local branch to withdraw or transfer funds to fraudsters*
    - *Prevent fraud taking place*
    - *Provide victim support to reduce the individuals future susceptibility to scams.*
    - *To arrest fraudsters*

- A key method employed by criminals committing fraud offences is to encourage the victim to attend their local branch in person to transfer money out of their account. It is not uncommon for the fraudster to accompany the victim. The Banking Protocol aims to ensure that all colleagues are able to recognise and have the confidence to question unusual transactions, and to provide a standardised process for managing these concerns and reporting cases to the police.

BANKING PROTOCOL PROCESS

If a customer is identified as making an unusual or out of character cash withdrawal or fund transfer request…

1. The colleague will discreetly question the customer about their withdrawal and the reason for making it.

2. If the colleague is concerned that the customer may be a victim of fraud, they will notify a senior member of staff and, where possible, take the customer to a quiet area or private room to ask further questions.

3. If the colleague believes the customer is the victim of fraud then they should call the police immediately on 999 quoting 'Banking Protocol'.

4. A police officer will be dispatched to the branch within 20 minutes (providing there's not a more serious incident to attend to).

5. The officer will speak to the branch colleague and customer. If an offence is suspected, the police will make efforts to arrest the suspect if possible.

6. The officer will provide crime prevention advice and reassurance to the customer.

7. The officer will also create a crime report, a report to Action Fraud, and a referral to social services if they believe the customer is vulnerable.

Success To Date

4354 ‘999’ calls made to the Police

£31.4M prevented from loss through the banking protocol

£7K Average prevention value per call

240 Arrests made

Case Studies

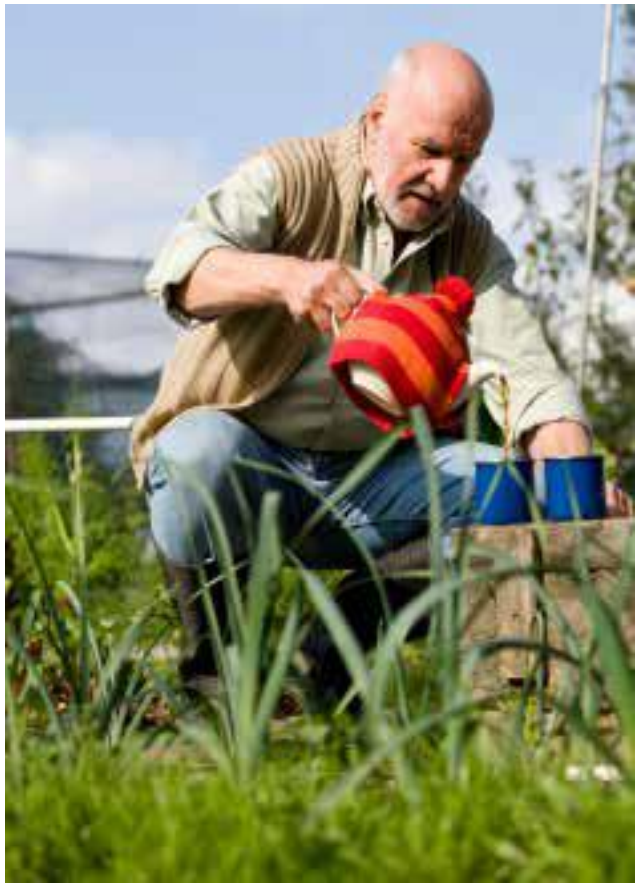
VICTIM PROFILE: 80 year old man

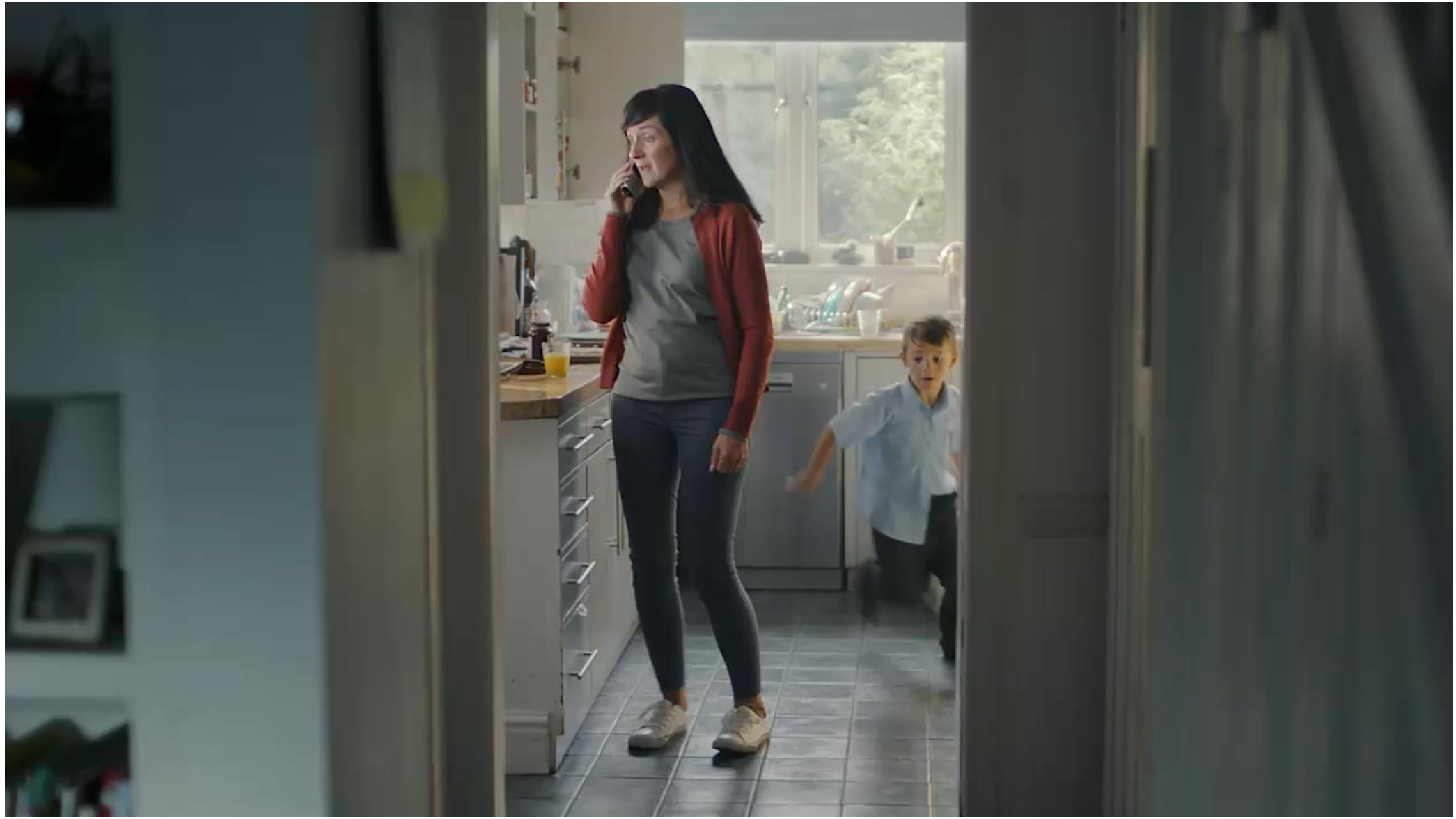
CASE: He received a call from an individual claiming to be from his bank (This individual was a fraudster). The Fraudster advised the man that they had noticed a problem with his account, which could now be susceptible to Fraud and he would need to transfer his money to a new safe account.

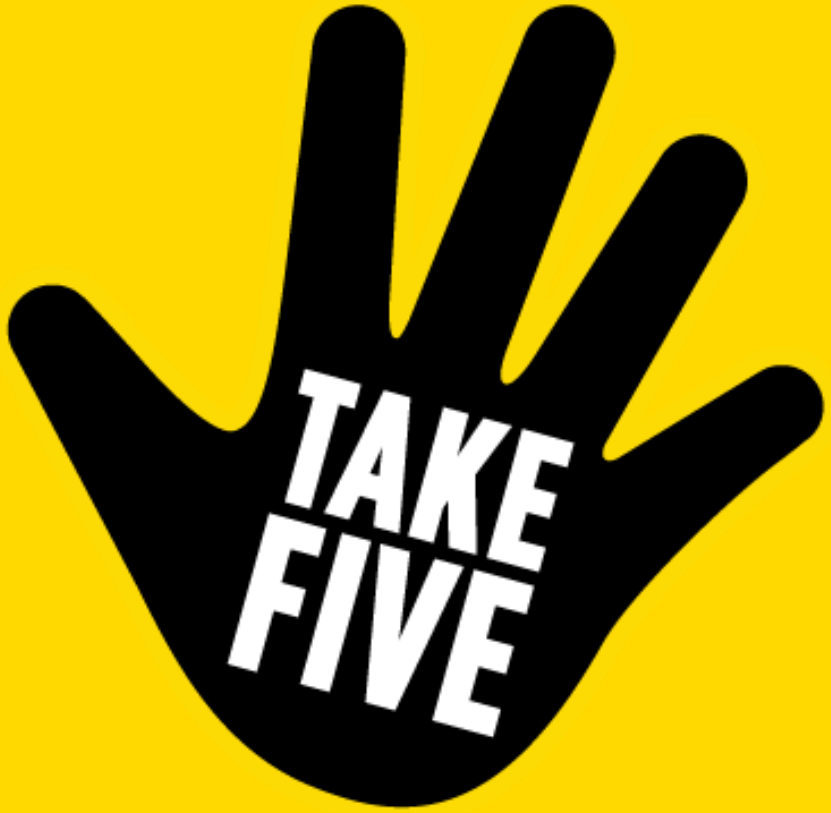
The Fraudster advised the customer to tell the bank staff he was transferring money to his son's account if asked, as one of the bank tellers were part of the scam.

The customer was wary, but more concerned about loosing his money so immediately went to his branch to arrange the transfer.

Branch staff has suspicions regarding the payment and took the man to a private room to ask questions. They discovered that the man didn’t even have a son and immediately invoked the Banking Protocol saving the man £30K.







TO STOP FRAUD™

THE TRUST REFLEX.

IT MAKES US LOSE CONTROL.

TAKE FIVE TO STOP FRAUD™

Take Five to Stop Fraud

- **Take Five to Stop Fraud** is a national campaign that offers advice to help everyone protect themselves from preventable financial fraud

- Phase 1 was launched by **Financial Fraud Action UK** (now part of UK Finance) in September 2016

- Phase 2 followed in September 2017, **backed by Her Majesty's Government** through the Home Office

- Phase 2 focussed on increasing customers' **confident challenge** to help them feel empowered to question potentially fraudulent situations, using the memorable phrase **'My money? My info? I don't think so.'**

TAKE FIVE TO STOP FRAUD™

The advice

STOP AND THINK

1. A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.

2. Don’t be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.

3. Always question uninvited approaches in case it’s a scam. Instead, contact the company directly using a known email or phone number.

TAKE FIVE TO STOP FRAUD™

The Take Five Voluntary Code

- To change customer behaviour towards fraud and scams and support the ongoing adoption of Take Five, the **Take Five Voluntary Code** will set out how signatories will provide **consistent and concerted use** of the campaign messages and logo throughout their **customer communications**.

- The Code will set out the **minimum expectations** required of signatories. These may include prominently displaying Take Five messaging in customer facing environments such as online.

- The Code will also include a best practice approach for **wider voluntary activity**, across a range of channels, for signatories to promote Take Five.

- The **central Take Five key message hub and campaign collateral** will provide the material required for signatories to implement the Code.

TAKE FIVE TO STOP FRAUD™

Find out more about Take Five by visiting

www.takefive-stopfraud.org.uk

TAKE FIVE
TO STOP FRAUD™