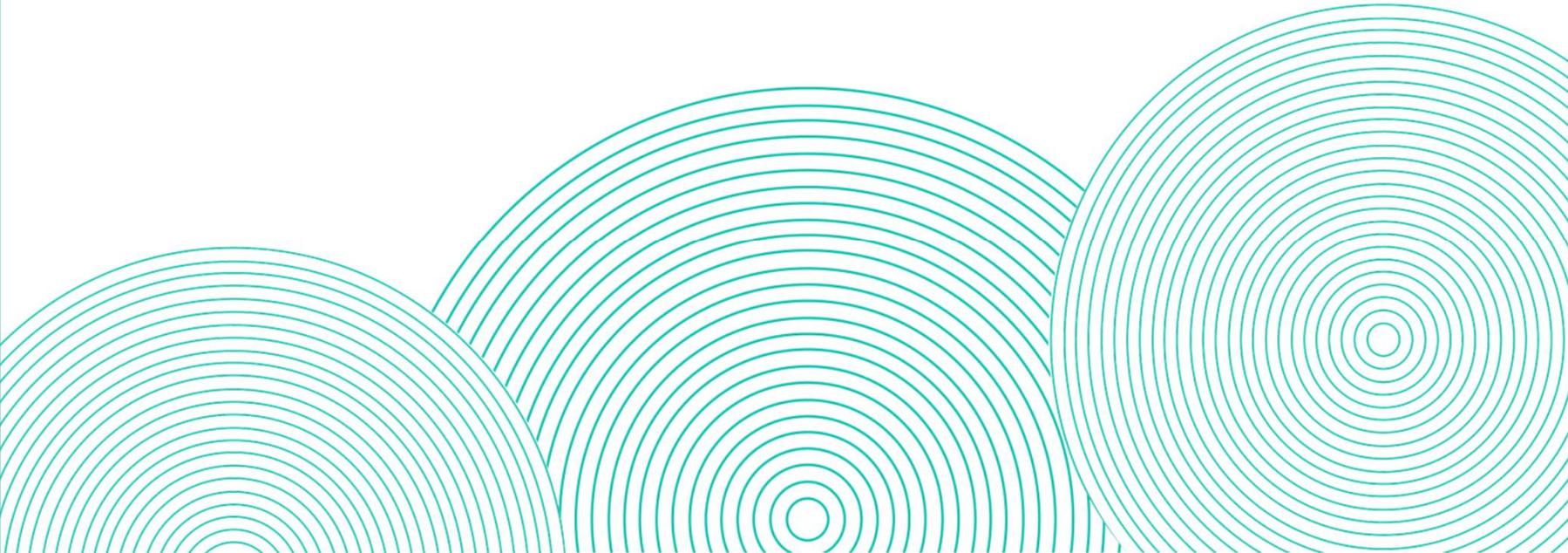


Financial Crime Customer Education and Awareness



UK
FINANCE



Consumer awareness and education requirement



UK
FINANCE

- PSF highlighted in its final strategy that a priority issue in financial crime is the ability of customers to identify and understand the methods by which criminals seek to exploit them to obtain or launder money
- Agreed customers need more information on steps they can take reduce the risk of becoming a victim or unwittingly participating in financial crime
- The strategy proposed a joined-up approach to consumer awareness and education
- It was identified that there was already a significant amount of activity underway to deliver awareness and education campaigns
- However these activities needed to be more co-ordinated and streamlined to improve clarity of messages and avoid unnecessary duplication

Current Landscape



UK
FINANCE

- A range of trusted organisations already deliver awareness on a range of fraud and scams – UK Finance, Home Office, FCA, GSOL, law enforcement, Cifas, Trading Standards, CAB, NHW, Crimestoppers
- Multi Agency Communications Group established and co-ordinated by CoLP Economic and Cyber Crime Unit with the aim of ensuring activities aligned, complimentary and consistent, and to encourage collaborative working and identify new MOs that require a focus
- Activities of participants cover a wide range of financial crime types including social engineering scams and ID fraud, phishing and online fraud, money mule recruitment, and investment fraud amongst others
- These reflect the priority areas highlighted by the PSF's Financial Crime Working Group
- A range of activities undertaken since the strategy established and planned going forward



TO STOP FRAUD

Take Five: Introduction & Overview



- Take Five represents the first time that all major banks and key financial service providers across the UK have come together to launch a national behaviour change campaign to combat financial fraud related scams. The initial campaign was funded solely by banks and aimed to overcome the trust reflex - calling for one simple action – to stop and think or in other words TAKE FIVE TO STOP FRAUD
- Phase 1 of the campaign was launched by FFAUK in September 2016 with a strong PR push and events held at London Waterloo, Manchester Piccadilly and Glasgow Central rail stations to promote the campaign and its messages.
- The campaign focussed on scams directly targeting customers, such as email deception (phishing) and phone and text-based scams (known as vishing and smishing), and was designed to remind people that it pays to stop and think.
- Members supported the campaign with in-branch activities and promotion through their communications networks including a high profile Take Five Day. Support from key stakeholders including Government, law enforcement, Cifas and others also contributed to the campaign's success which saw widespread coverage across TV, radio, national print, online, and social media.
- After launch, each month the campaign focused on different themes to raise awareness and change the behaviours of priority audiences. Activities included a partnership with the British Chambers of Commerce aimed at 5,000 businesses with messages such as those around invoice fraud.
- 27% of people recall campaign. 65% of people said they would behave differently following exposure to campaign messaging.
- Phase 1 of the campaign shortlisted for PR Week Award, finalist at the SABRE Awards and a winner at the PRCA City and Financial Awards.



Take Five: Phase 2



UK
FINANCE

- Building on Phase 1 the focus of Phase 2, launching in early October, is to help customers feel empowered by questioning potentially fraudulent situations – establishing increased levels of “**confident challenge**” amongst **defined target groups** in scenarios where they are at risk of being scammed i.e. being asked for security details, clicking on links, requests to take action (such as moving money, providing remote access to their PC or responding to unexpected refund offers).
- A new call to action has been developed for Phase 2 – **My Money? My Info? I Don’t Think So**
- Working with the Home Office’s behavioural change team two target audiences have been identified. The priority audiences are based on RICUs Serious and Organised Crime Prevention Segmentation model and Mosaic profiling. Together these groups comprise 12m adults:
 - **Primary (core focus for paid media):** C1, a naturally trusting personality makes them vulnerable to fraud and scams. High propensity for behaviour change. Three demographic sub-groups Under 35s, Men aged 35+ and Women aged 35+ in a relationship (*this group are particularly important, as they also have a role to influence others*)
 - **Secondary (core focus for partnership activity):** E, older, 45-65, often couples plus those 65+. A lack of awareness of Serious and Organised Crime and unwilling to challenge others makes this group vulnerable. Reliance on ‘trusted sources’ makes them especially receptive to partnership marketing.
- The campaign will be focussed around three key peaks of activity each tackling different types of fraud and scams. Each peak will be comprised of PR activity, paid for digital and radio advertising, partnerships activity and work with key influencers as well as digital content and social media activity. Banks will continue to support the Take Five campaign through their customer communication channels including a Take Five Week planned for early 2018.
- Toolkit of Take Five collateral available for stakeholders to promote campaign messages available from www.takefive-stopfraud.org.uk



TO STOP FRAUD™

Take Five: Phase 2



UK
FINANCE



A genuine bank or organisation will never contact you asking for your PIN, full password or to move money to a safe account. Don't give out personal or financial details.

takefive-stopfraud.org.uk



TO STOP FRAUD™

Other Campaigns and Areas of Focus



JUN 2017		PASSWORDS 19th		PROTECT/CONNECT 17th to 25th		
		AUTO FRAUD 17th		SCAMS AWARENESS MONTH		IDENTITY THEFT (CORP COMMS) TBC
JUL 2017		SPOT SOMETHING PHISHY 27th				
		SAFE SOCIAL MEDIA 21st		INTELLECTUAL PROPERTY (CORP COMMS) TBC		CYBER CHOICES II TBC Aimed at informing teenagers of the consequences of hacking etc.
AUG 2017						