“Banks are leaving customers wide open to spoofing fraud” Answer Pay responds

Which? The consumer champion has claimed that banks are failing to protect their customers and are “leaving customers wide open to spoofing fraud”. Their investigation found that high street banks representing over 60% of the UK consumer banking market had not taken advantage of the latest technology such as Ofcom’s “Do Not Originate” registry which prevents spoofing of important phone numbers.

Only last week the Metropolitan Police announced the closure of iSpoof who were trying to defraud customers by impersonating banks including Barclays, Santander, HSBC, Lloyds, Halifax, First Direct, Natwest, Nationwide and TSB. The police report that “At one stage, almost 20 people every minute of the day were being contacted by scammers hiding behind false identities using the site”.

Pay.UK, who govern the UK’s Faster Payment service, introduced a framework for Request to Pay in 2020. This meant that banks didn’t have to rely on insecure channels like email and SMS where customers can’t trust the identity of the originator. Instead communications could be transmitted securely bank app to bank app where participants had been through a “Know Your Customer” process to validate their identity.

Answer Pay were the first certified provider of Request to Pay technology, Mike Chambers Chairman of Answer Pay comments:

“We see Request to Pay as a vital tool in helping to secure remote payments but we can’t do it alone, the financial services industry has to respond to the fraud challenge before us.”

Given the lack of adoption and eye watering fraud on its network, we call on Pay,UK to take the required steps to amend its rules to ensure the benefits of Request to Pay are realised, by compelling users of its faster payment service, such as banks, to deploy the service.

The fraud problem we have in the UK is so bad that UK Finance have described it as a “national security threat” following the 123% increase in impersonation fraud last year. Surely regulatory intervention is needed to ensure that the appropriate steps are taken. There is a precedent for regulatory action in other markets with the Monetary Authority of SIngapore outright banning banks from sending clickable links in SMS and email instead promoting app to app communication.

Perhaps all is not lost then, with new regulatory powers expected to be granted by parliament to the Payment Systems Regulator we should hopefully see Faster Payments become a safer way to transact with the effective use of Request to Pay.