Feature

KEY POINTS

- There is nothing in the regulatory regime applying to mobile network providers which requires them to undertake due diligence enquiries on their customers so as to ensure that they are seeking to have access to the mobile telephone network for legitimate purposes.
- The content of communications will be regulated, if at all, in accordance with the specific regulations governing the content provider itself (the bank).
- The key to reducing the vulnerability of M-banking to abuse by the criminal fraternity lies on the banks ensuring that their security and due diligence requirements are effective and reflect best practice.

Authors Jonathan Fisher QC and Shaen Catherwood

Abusing M-banking for money laundering: an unregulated activity

This article considers the application of UK and European money laundering and electronic communications legislation to prevent the abuse of M-banking (banking through mobiles).

With the extraordinary advances in electronic technology – the 4G mobile network auctions having recently taken place, it is possible for customers to undertake almost all their banking transactions by using a mobile telephone ('M-banking').

The opportunities for criminal abuse of this facility are enormous, it being far more difficult for the enforcement authorities to trace the user of a mobile telephone than the user of a fixed line telephone or broadband connection. Today, 'carousel fraud', also known as 'MTIC fraud', causes the HM Revenue & Customs (and us, as taxpayers) to lose approximately £3bn each year as a result of fraudulent transactions involving the purchase and sale of electronic goods subject to Value Added Tax, with the fraudsters giving instructions in relation to these transactions and movement of monies using Pay As You Go mobile telephones, either acquired in false names or stolen from their rightful owners. Unquestionably, the use of M-banking for money laundering purposes will almost certainly grow as the 4G mobile network offers the fraudsters a better banking service through which to pursue their criminal activities.

Although the greater use of mobile telephone technology swells the profits made by the network providers, the use of the mobile telephone network by the criminal fraternity for M-banking will be an unwelcome development since it brings in its wake a host of unanticipated problems. Network providers have already encountered some unpleasant experiences, not so much with the use of mobile telephones for M-banking, as with the fraudulent use of mobile telephones more generally. One particular type of fraud, known as Wangiri fraud, has gained sufficient prominence to justify its own entry on Wikipedia! The internet encyclopaedia explains that Wangiri fraud originated in Japan and is a scam which involves a computer using hundreds of phone lines to dial mobile phone numbers at random. The numbers appear as missed calls on the recipients' mobiles. Believing a legitimate call was cut off, or simply curious, users are enticed to call back. The numbers are either premium rated, based abroad or contain advertising messages. The fraud operates by causing the owner of the mobile telephone to incur significant charges which he must pay his network provider, with a proportion of this charge being passed to the fraudster as commission earned from generating the call to the premium rated line (or some other line) which he set up when equipping himself with the tools to commit the fraud. Less sophisticated mobile telephone frauds will involve the theft or hijacking of a mobile telephone which is used by a criminal at the owner's expense.

There are interesting issues arising here relating to the application of Pt 7 of the Proceeds of Crime Act 2002. By virtue of their involvement, questions can be asked as to whether the mobile network providers become exposed to liability for the commission of a money laundering offence where, for example, they retain in their possession monies generated by criminal activity, and also whether, under Part 5 of the same Act, the network providers are vulnerable to an action for civil recovery to disgorge any criminally obtained monies they may be holding. But more to the point with regard to the problems posed by M-banking, there is nothing in the regulatory regime applying to mobile network providers which requires them to undertake due diligence enquiries on their customers so as to ensure that they are seeking to have access to the mobile telephone network for legitimate purposes and not for furthering a fraudulent or some other criminal activity.

THE REGULATORY REGIME

At first blush, the regulatory regime's silence is strange when contrasted with customer due diligence requirements imposed on those operating in the financial sector, such as banks and solicitors. The reason for this silence is explained by the efforts made by Parliament to ensure that the regulatory regime for mobile network operators is a 'light touch' one, to facilitate competition both within the UK and with foreign competitors. The Communications Act 2003 is the principal legislation governing the regulation of electronic communications networks and services; through the medium of OFCOM, its jurisdiction encompasses not only telecommunications, but also the internet and broadcast media. The use of a mobile telephone network for M-banking falls within the remit of the Act and OFCOM's jurisdiction only in the broadest sense. OFCOM regulates electronic communications networks, defined in s 32 as the physical system used for the conveyance of signals, and also electronic communications services, which consist of the conveyance of the signals on a network. The provision of the actual material which is to be conveyed amounts to a 'content service' which will fall directly within OFCOM's jurisdiction only to the extent that it is a premium rate service, or to the extent that it involves criminal misuse of the network, for instance if it is grossly offensive for the purposes of s 127(1). An M-banking service consists in part of a content service in so far as it provides, say, the website or app by which a customer obtains access to a bank account or other related services; the bank and its customer are also consumers of an electronic communications service which the mobile network provider has provided. However, in

Biog box
Jonathan Fisher QC and Shaen Catherwood are barristers practising from Devereux Chambers, London.
Email: fisher@devchambers.co.uk and catherwood@devchambers.co.uk

neither context is the M-bank likely to attract the attention of OFCOM.

Unlike the Financial Services Authority, for example, OFCOM has not imposed any regulatory requirements on mobile network providers to take steps to prevent their networks' or services' use for the purposes of criminal activity. OFCOM's principal duties, set out in s 3 of the Communications Act 2003, are to 'further the interests of citizens in relation to communications matters' and 'to further the interests of consumers in relevant markets, where appropriate, by promoting competition'. The social and economic benefits of communications services, and the importance of a competitive and diverse communications market, are fundamental to the European and national legislative framework. So whilst OFCOM must have regard, amongst other matters, to 'the desirability of preventing crime and disorder', this goal must be understood in the context of a relatively light touch regulatory regime which is designed to remove barriers to the entry of undertakings into the European electronic communications market. Indeed, s 6 of the Act expressly requires OFCOM to review its functions in order to ensure that its regulatory regime does not impose or maintain unnecessary burdens. The European dimension is very significant. There are five European Directives (the Framework Directive (2002/21/EC), the Universal Service Directive (2002/22/EC), the Access Directive (2002/19/EC), the Authorisation Directive (2002/20/EC) and the Directive on Privacy and Electronic Communications (2002/58/EC). These Directives are concerned primarily with issues of competition, freedom of choice, technological diversity, and quality of service. As far as the conditions applicable to the operation of mobile networks are concerned, the Authorisation Directive is the main instrument to consider, and with potential application to M-banking it permits the imposition by member states of restrictions in relation to the transmission of illegal content (art 9), conditions enabling the legal interception of communications (art 11) and conditions relating to the prevention of unauthorised access to public networks (art 16). However, there is no reference in this or the other Directives to the imposition on operators of conditions requiring the prevention of crime, analogous to those found in the financial services sector.

As regards OFCOM, these limitations on stringent operating conditions, such as an obligation to perform customer due diligence or put in place measures to detect the criminal use of the mobile telecommunications network, are reflected in s 45 of the Communications Act 2003. This limits OFCOM to setting (a) general conditions which apply to all operators and which can only cover certain matters (essentially those set out in the Authorisation Directive), and (b) conditions applicable to specific operators, but only to the extent that they relate to certain itemised matters such as the provision of a universal service and the exercise of significant market power. That said, it is right to record that in the most recent version of the general conditions issued by OFCOM dated 30 July 2010, Annex 1 to General Condition 14 obliges Originating Communications Providers (ie: those providing call originating services to consumers) to provide certain information to consumers, including information concerning the avoidance of scams relating to the abuse of premium rate services. But the provision of this sort of information in relation to the abuse of M-banking would be an entirely different matter. Whereas the information here is provided to protect the customer and the mobile network provider against sustaining losses through the fraudulent use of the telephone service, in the case of M-banking it is only the bank which loses out as the victim when it executes instructions which further a criminal cause.

In short, mobile network operators are regulated in respect of the networks and transmission services they provide; with the principal exception of premium rate services, the content of communications will be regulated, if at all, in accordance with the specific regulations governing the content provider itself.

MONEY LAUNDERING REGULATIONS

Consistently with this, as the law presently stands, mobile network providers do not fall within the regulated sector for the purposes of the Money Laundering Regulations 2007. They are not "financial institutions" within the meaning of regulation 3(3) of the Regulations and there is nothing to suggest that the Third European Council Directive on Money Laundering was ever intended to apply to them. This is perhaps not surprising, since unlike banks and professional advisers such as solicitors and accountants, mobile telephone network providers could not properly be described as gatekeepers to the financial system. More accurately, the network providers operate a service which enables criminals to use an instrumentality of crime, namely, a mobile telephone. Also, in terms of practicality, any customer due diligence enquiries would need to be undertaken at the time when the mobile network provider makes the contractual arrangement with its customer. Invariably, this contract is made in a retail outlet where the retailer acts as an agent for the network provider or directly when an arrangement is made over the internet. To impose the obtaining of customer identity and 'know your client' documentation in either situation would be unrealistic and serve only to generate unnecessarily a mountain of paper which would almost certainly not contain a scintilla of good quality criminal intelligence. Mobile telephone network providers could also point out, with reference to the particular concerns of criminality posited by M-banking, that whilst M-banking is able to abuse the mobile telephone network, precisely the same nefarious activities can be performed more comfortably on a computer. There is no logical distinction to be drawn between an internet provider and a mobile network provider in this regard, and if mobile network providers were to be brought into the regulated sector, all internet providers – and agents acting on behalf of internet providers when introducing customers to their internet provider – would need to be afforded equivalent treatment. With the coalition government committed to reducing the regulatory burden, this suggestion is not likely to find favour with anybody apart, perhaps, from the banks.

In this context, it needs to be remembered that the banks are obliged to undertake due diligence enquiries on their customers before affording them banking facilities. Hence it would seem that the key to reducing the vulnerability of M-banking lies in imposing greater regulatory burdens on the banks to ensure that their security and due diligence requirements are effective. ■