Selina Chadha
Consumer Policy Director, Ofcom
Direct line: 020 7783 4147
Email:
selina.chadha@ofcom.org.uk

29 October 2018

Open letter to Mobile Communications Providers

RE: Mobile Switching Reforms – authentication on the SMS Auto-Switch route

I am writing in response to concerns raised by some Mobile Communications Providers in relation to their obligation, under Ofcom's Auto-Switch reforms, to respond to an SMS PAC/N-PAC request within 60 seconds, and their ability to authenticate customers within this time period. Some providers have raised concerns that the SMS route would increase fraudulent activity and they requested a change to General Condition C7.28 to address this.

The relevant provision of the General Conditions states:

C7.28 Regulated Providers must ensure that when they provide the PAC or N-PAC and/or (as applicable) the Switching Information in accordance with Condition C7.26 (a) and (b) to the a Mobile Switching Customer, they do so no later than one minute from receipt of the request, save that, in the case of a request made by phone, the SMS required under Condition C7.26(b) may be sent at the latest up to one minute from the end of the phone call.

We note that authentication concerns were raised in response to our May 2017 Mobile Switching Consultation, and we responded to these points in our December 2017 Mobile Switching Statement (see paragraphs 4.106 to 4.110 A2.55 to A2.72). We have further discussed these concerns with providers at several roundtable meetings on the implementation of the reforms. Following the 17 September 2018 industry meeting, we asked providers to individually write to us setting out their position on the issue. We have now considered those letters.

We have also received advice from the ICO that any data security measures that are put in place to authenticate a customer should be proportionate to the risks. That assessment of risk involves consideration of that data being used fraudulently or sensitive data getting into the wrong hands. We discussed with ICO that some personal data is more sensitive than others (e.g. health data compared to a PAC).

In our view, the risk of fraud on the SMS Auto-Switch route is low and represents an improvement on the current PAC system. We note the following factors are likely to serve to reduce the risk of fraud:

1. ***The requester must be in possession of a SIM to request the PAC/N-PAC which provides a level of authentication, i.e. the PAC/N-PAC is going to the account holder.*** Under Auto-Switch, to use the SMS route a requester must be in possession of the handset/SIM itself (this is not the case for requests made online or by phone). A fraudulent SMS PAC/N-PAC request would therefore have to either be carried out by someone close to the victim, who could gain access and knows the device PIN (and could presumably bypass other forms of security check) or someone who has stolen the handset. The need to be in possession of the handset therefore reduces the likelihood that someone other than the authorised account-holder can request the PAC/N-PAC.

2. ***Multi-SIM accounts are excluded from the SMS route.*** Some providers raised concerns over family members porting numbers or cancelling services without the authorisation of the account holder, where they are part of a multi-SIM arrangement. As we clarified on 22 March 2018, multi-SIM accounts are excluded from the SMS route and therefore this risk does not exist.

3. ***The port takes up to 24 hours to take place.*** For a number to be ported, the PAC has to be redeemed (i.e. obtaining a PAC in itself does not do anything). The actual port of the number takes one working day to complete. In the case of theft, a victim would therefore have up to 24 hours to notify their provider of the stolen handset, giving them time to prevent the port from completing.

4. ***Businesses are excluded from the requirement to provide a PAC/N-PAC via the SMS route within 60 seconds of request.*** Several providers raised concerns that there could be instances where a PAC/N-PAC is requested by a phone user who is not the authorised account holder (e.g. an employee whose company provides them with a mobile phone). However, we note that providers of business tariffs have two days to respond to an SMS PAC/N-PAC request, which would give them plenty of time to verify the requester.

5. ***Flagged numbers or accounts.*** Where a fraudster may be targeting the number itself, as in the case of 'golden numbers', or a provider considers there to be an increased risk of fraud, we understand that providers put flags on these numbers or accounts. We consider that this should affect a very limited number of customers and in these cases, it may be reasonable for providers not to provide the PAC-N-PAC via the SMS route on the basis of an appropriately assessed risk of fraud. We also think golden numbers are more likely to be used by businesses and so are likely to be excluded by the text route under Multi-SIM and business exemptions.

We note that there is at least a theoretical possibility that someone known to the authorised account holder, who is not covered by the Multi-SIM exemption above, may want to maliciously switch their service (i.e. to incur ETCs). However, it appears to us that these instances are likely to be very rare. We also note that such a person may know enough about the authorised account holder to bypass other verification methods (i.e. online or phone routes). In any event, this very limited number of theoretical incidents do not seem to us warrant modifying our reforms to the detriment of the many consumers who will benefit from an easier and simpler method of switching.

Inclusion of additional authentication information in SMS PAC/N-PAC request

It is for providers to determine how best to satisfy the requirements of the General Condition and data protection regulations. It therefore remains open to them to design their processes to include additional authentication of requesters, as long as these steps do not put them in breach of their regulatory requirements under the General Conditions.

We note that during discussions with industry a process was suggested by which consumers would be required to include certain information in the initial PAC/N-PAC request by which they could be further authenticated.

As we explained at our meeting of 17 October, we consider that this would in principle be compliant with the GC, as long as the information required did not lead to an unacceptable level of failed SMS requests. This is more likely to suggest information that is easily accessible or memorable to the customer and the need for it to be provided to be clearly displayed on the providers' website and other consumer-facing information. In other words, the additional authentication requirement should not be a barrier to ensuring that switching is made easier and simpler for consumers in accordance with Ofcom's policy objectives when it mandated the reform to mobile switching processes. We will be monitoring the failure rates of the PAC/N-PAC SMS request route to ensure any additional authentication requirement is not a barrier to switching.

Summary

For the reasons set out above, we are not minded to make any changes to General Condition C7.28.

We look forward to continue working with industry to ensure that consumers fully benefit from these reforms by the implementation date of 1 July 2019.

Yours sincerely,

Selina Chadha