STRONG CUSTOMER AUTHENTICATION

On September 14th 2019, additional security to protect online payments, known as *Strong Customer Authentication*, will be introduced across Europe as part of the Second Payment Services Directive (PSD2) (for more information on PSD2 follow this link on the Banking and Payments Federation Ireland website: https://www.bpfi.ie/key-topics/psd2-coming-ready/). In order to support these additional security requirements, online accounts on Kilcloon Credit Union's Online Banking Website and Mobile App services will be upgraded to include Strong Customer Authentication (SCA).

What is PSD2?
PSD2 was introduced to improve security, reduce fraud and encourage competition, while taking into account modern payment methods such as mobile payment and online payment.

What is Strong Customer Authentication?
Strong customer authentication (SCA) is authentication based on the use of two or more elements, namely:
1. Knowledge - something only the user knows. For example, a password;
2. Possession - something only the user possesses. For example, a mobile phone;
3. Inherence - Something the user is. For example, fingerprint or iris pattern.

How will this affect Kilcloon Credit Union's Members?
- Whenever a member logs in to their online account, they may be asked to take an additional step to further authenticate themselves. This will happen every 90 days.
- When a member sets up a new payee they will be asked to provide further authentication.
- If a member wishes to view transactions or documents older than 90 days, they must provide further authentication.

How will Members provide the additional authentication?
Where a member has the Mobile App installed, an authentication code will be delivered via the app. When using a laptop or PC, an SMS containing the code will be sent to the member's phone.

When will these changes be implemented?
Strong Customer Authentication days will be implemented on by no later than September 14th 2019.

Are there any other impacts from SCA?
Third party card issuers and merchant service providers are also likely to roll out their own SCA solutions in relation to transactions on credit union accounts, but these providers will issue their own announcements and instructions in due course.

Is SMS safe?
In general terms, SMS does have some inherent weaknesses, however, through our systems service provider we have sourced a robust security solution which protects the SIM cards in mobile phones from 'hijacking' (SIM Swap attack). This solution, *SIM Swap Protection Service,* is used by all the leading banks in Ireland, so we are confident it is entirely suitable for online account users.

It should also be noted that the European Banking Authority ('EBA') has indicated that SMS is a valid medium for the transmission of authentication codes and one-time passwords ('OTP') as long as the SMS is subject to measures that prevent replication of the SIM.