# Cambridgeshire Police Fraud alert -
# Bank text scam with genuine card details…..

I wanted you to be aware of a convincing text and phone scam, involving potentially genuine bank card details that will be recognisable by the text recipient. I suspect, that criminals will have come into possession of stolen data including the last four digits of a bank card and an associated mobile phone number, not enough to steal your money, but by contacting you and pretending to be your bank, they may just deceive you into giving them the additional card information they need to commit fraud.
The scam appears to go as follows; my comments are in brackets.

The recipient received a text message similar to; 'You will shortly receive a text message from Lloyds Bank to confirm recent activity on your account' (The recipient is actually a Lloyds bank customer. Remember, if criminals have parts of your bank card, they will work out the issuing bank)

This is followed up by a second text stating 'Your Lloyds Credit card ending in #### (They gave the correct 4 numbers) was used on 13-09-2020 17:18:50 at Grand Metro for £2269.18. This payment was declined. If this was you reply YES, otherwise reply NO. There is no need to call us. Responding to this text is the quickest way to update your account.
(The criminal invites you to reply whether it is Yes or No, by replying you are telling them that you have received the text and that you may have taken the bait. Also note, they say responding by text is the quickest way to update your account, this should read this is the best way we can steal further information and your money. I would expect a genuine bank text to say something like, 'if it was you, do nothing. If it wasn't you, contact your bank'. Do not click on any link or contact the telephone number quoted in the text or any communication. Use your previously tried, tested, and trusted method for contacting your bank. Remember as well, by the second text the criminal will have installed some kind of fear, anxiety and stress into recipient making them possibly more vulnerable to falling for the scam)

This second text was followed by a phone call with the caller talking about fraud and inviting the recipient to press various numbers on the keypad, it was at this point the recipient of the call put the phone down. The criminal rang several times over the next couple of days, each call preceded by a text.
(Avoid pushing any numbers on your keypad during a telephone call in which you don't recognise the voice of the caller or it is automated, this could result in a range of problems including being diverted to a premium rate telephone number and you will be charged a lot of money per minute)

The recipient then contacted their bank and on this occasion no money has been taken, but the bank confirmed it was a scam.

**STOP** - Taking a moment to stop and think before parting with your money or information could keep you safe.
**CHALLENGE** - Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
**PROTECT** - Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

Any non-urgent questions or concerns please contact me.

Mr Nigel Sutton 8517
Cyber Protect Officer
Serious & Organised Crime (Intelligence and Specialist Crime Department)
Cambridgeshire Constabulary