Don’t block scam texts, say banks

As phone giants fail to tackle fraudsters, customers are being told that barring messages will stop them accessing their cash

Ali Hussain

October 21 2018, 12:01am, The Sunday Times

Carol Dix had a narrow escape but still wants to know: ‘How did they hack into the Santander text-message thread? ’BEN CAWTHRA

Bank customers who are bombarded with hoax text messages from fraudsters have been told not to block them — because doing so would also stop them seeing genuine messages from their banks.

Crooks have found ways of sending text messages that appear almost identical to those sent legitimately by banks. Crucially, the texts appear in the same message thread on customers’ phones as genuine texts sent previously by the banks.

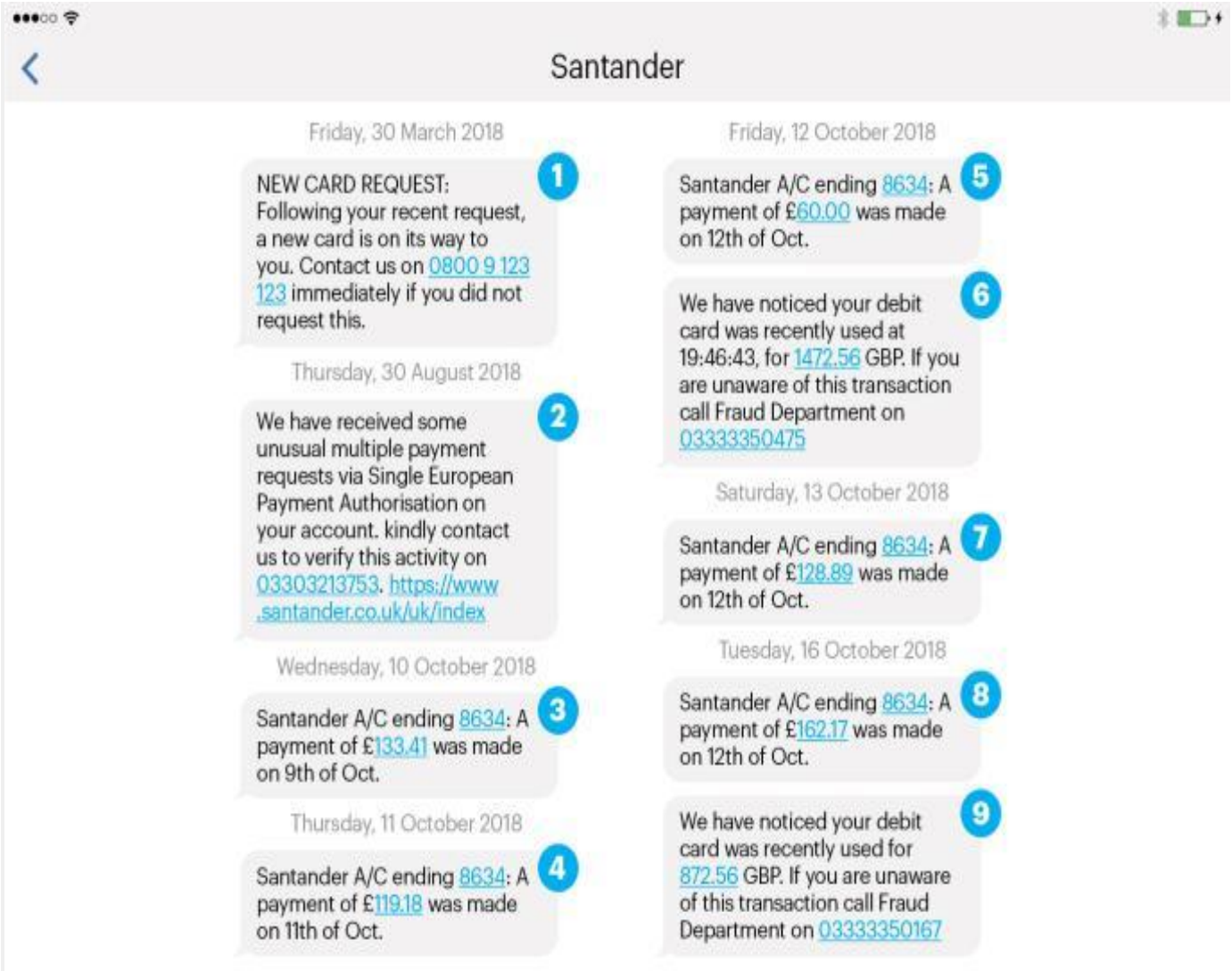
Most financial institutions communicate with account holders by text message — such as to ask them to confirm an unusual payment or to notify them of an online transaction.

However, customers of Royal Bank of Scotland, whose brands include NatWest; Lloyds, which owns Halifax and Bank of Scotland; and Santander also send single-use passcodes by text. This happens when, for example, they want to make a payment to someone new or change direct-debit details online.

The banks' high street rivals supply devices that generate the codes, leaving customers able to block texts — via their phone settings or apps — without hampering their banking services.

The banking industry says it is working with telecoms companies to block fraudulent messages, which are sent in an effort to make victims transfer money to bogus accounts. However, Money understands banks and the police are increasingly frustrated because they feel phone operators are doing little to stop it.

"At times it feels as though the telecoms industry is not on the same page as the banks on this," said one senior bank official. "We need a more concerted effort by the mobile phone industry and the regulator to stamp out this practice."



Carol Dix received these texts, but can you tell which were from a fraudster? (See below for answers)

Carol Dix knows the lengths scammers will go to. In March, Santander sent her a new debit card after spotting unusual activity on her account.

Then, on August 30, she received a text message apparently from Santander alerting her to “unusual multiple payment requests” on the account. The text was on the same thread as messages she had previously received from the bank

Dix, from Dollis Hill, northwest London, said: “It was good to think the bank was keeping an eye on my account.”

The message instructed her to contact the bank’s “fraud department”, which she did immediately using a number given in the text.

Her call was answered by a woman who knew precise details about her account balance and transactions. The woman said that three large payment requests from Belgium were set up to leave her account by midnight. “Naturally, she had me panicked,” said Dix.

However, Dix, 71, became suspicious when told to transfer funds to a “safe account”, which the woman said had been set up for her. At that point, she put the phone down. “I actually apologised for being rude but said I had to check it out with my branch.”

Staff at the branch told Dix, a former journalist, that the text and call had indeed been part of an attempted fraud.

“I’ve had a narrow escape but questions remain,” she said. “How did they hack into the Santander text-message thread? How did they seem to know how much I had in my account?”

Twelve days later, Dix received another text asking her to call Santander. Again, this appeared in the same thread as genuine bank messages. She did not respond, fearing scammers again. Four days later, more bogus messages arrived.

Santander confirmed the texts were fraudulent — but it urged her and other customers not to block them, saying that if they did, “they would also block all legitimate texts from us”.

The bank added that conmen can “spoof” a phone number so that it appears that messages are from the bank.

“Sadly, scam texts can appear in the same thread as genuine messages from your bank . . . If a customer is asked to call their bank, they should use the

number on the back of their card to be sure they are speaking to the right people, and not a scammer."

Santander said customers should not panic or allow themselves to be rushed into following instructions in a text, and added that it would never ask people to transfer money or disclose their account details or passcodes.

This advice applies to customers of all banks. However, there are no hard and fast rules for how to spot a fake text message. If you suspect that one may be from a fraudster, call the bank using the number on the back of your card to check if it is genuine.

NatWest said: "We would not advise customers to block the number, as it may prevent them from receiving genuine messages from their bank." It pointed out that its customers can still access their accounts without the passcodes, but they are not able to set up new payees.

UK Finance, which represents the banking sector, said: "Many of the solutions to this issue lie outside the financial sector, which is why the industry works closely with network operators, government and other industry stakeholders.

"We are working to build on previous successes of joint work with the telecoms industry to mitigate this threat."

City of London police, which oversees the national anti-fraud strategy, said: "It is important that telecommunications companies dedicate time and resources to fraud prevention.

"We will continue to work with them to disrupt phone lines and, where possible, support them by sharing intelligence to help prevent fraudsters from operating in this area."

Ofcom, the telecoms regulator, acknowledged that more work needed to be done. "We're working closely with the financial authorities and the mobile providers to find a preventative solution to this global problem," it said.

Answers: 1 Real **2** Fake **3** Real **4** Real **5** Real **6** Fake **7** Real **8** Real **9** Fake