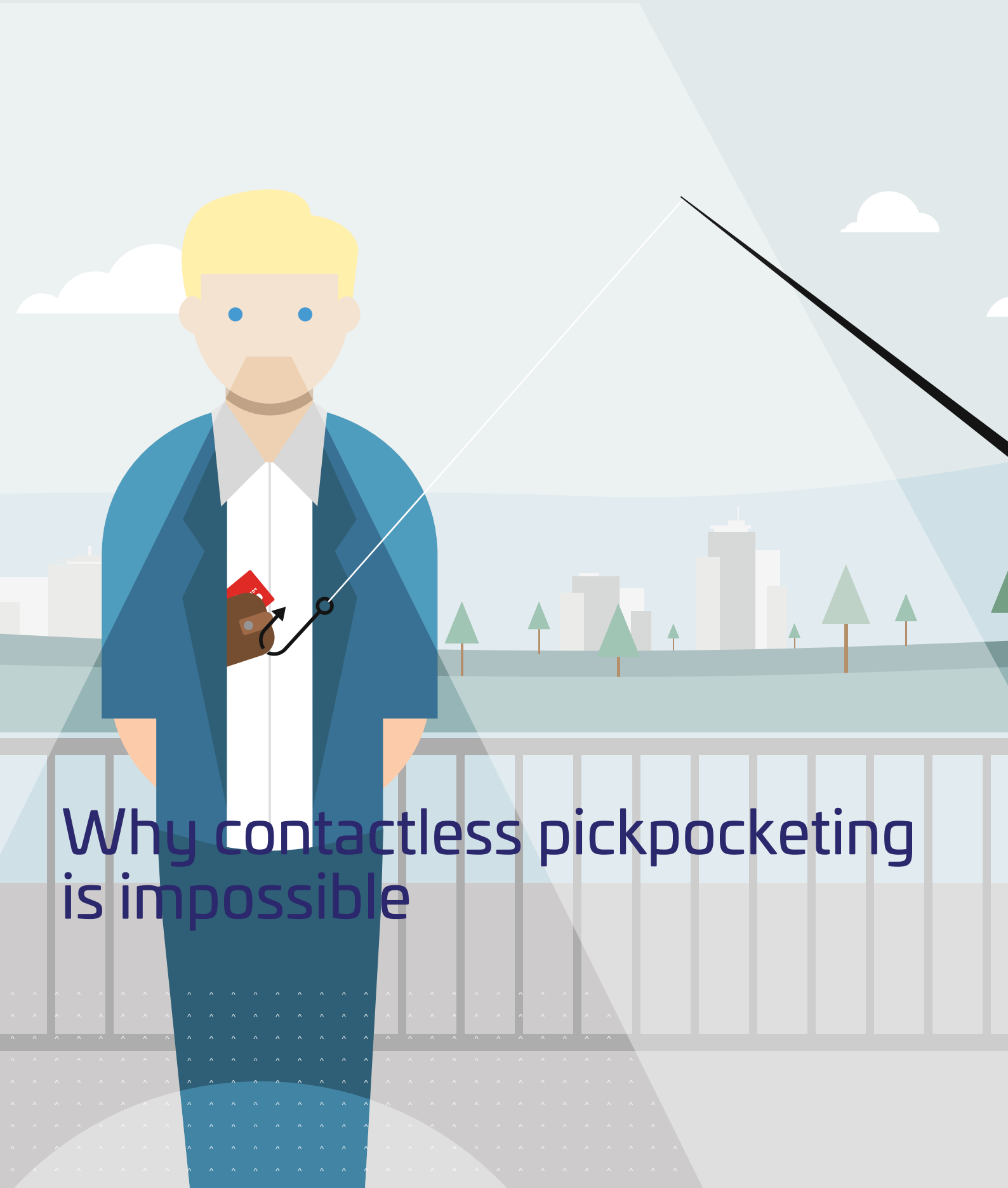
thalesgroup.com

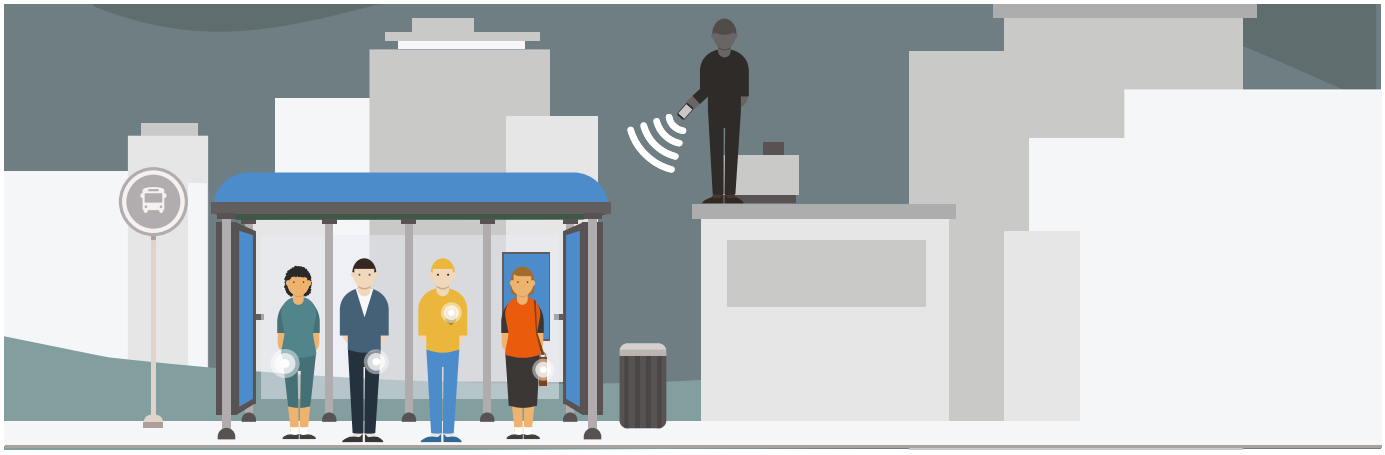
THALES



Why contactless pickpocketing is impossible

Why contactless pickpocketing is impossible

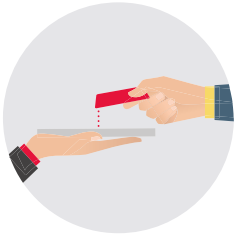
Banking & Payment Services



The myth: Data theft with long-range RFID readers

This myth says that fraudsters would be able to use long-range RFID readers to extract data from contactless cards from a large distance, and use that card data to access cardholders' accounts and steal money.

«NFC communication works only within a very short range (4 cm max)»



The NFC antennas can communicate at maximum 4 cm.

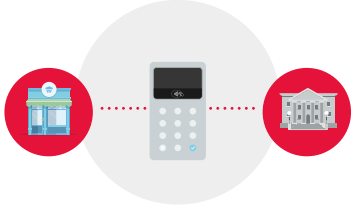
The reality

No, it is not possible to use long-range RFID readers to extract data from contactless cards. The near field communication (NFC) technology in contactless cards uses a 13.56Mhz radio frequency technology that only transmits digital data within a very short range. Typically the optimum distance is 4 centimeters or less - beyond the signal is rapidly decreasing and can never exceed 10 centimeters. No communication can be performed beyond that short range.16K/36K/72K EEPROM available*

The myth: Contactless skimming with close range readers

According to this myth, a fraudster equipped with an NFC reader would be able to access contactless cards in someone's pocket or bag in crowed public spaces like in the subway. By doing so, the myth says they would extract enough sensitive data to make a counterfeit card or make online purchases.

«Fraudsters will not succeed to extract enough relevant information to counterfeit a card»



Every POS terminal is registered to a merchant and a bank.

The reality

No, it is not possible to clone a contactless card thanks to data collected by a hidden reader like a smartphone or any other NFC reader.

It is also impossible to collect enough data from the card to complete an online purchase.

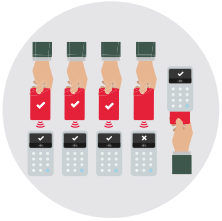
Only a genuine POS, provided by an acquiring bank, is capable of communicating with the card – and a fraudster using a genuine POS would get caught by the aquiring bank and processing network.

In contactless mode, key data such as card-holder name are blocked, meaning that any attempt to skim data from a contactless card would access less key data than can be read of the front of a card, and much less than is accessible from a magstripe.

The myth: Large losses with stolen card

Because low value contactless transactions can be made without requiring a PIN code, this myth says that a thief could spend large amounts of money through many repeated small purchases.

«The number of contactless transactions that can be performed once a card is lost is very limited»



After a certain number of contactless transaction, a chip and pin reset is required.

The reality

No, even with a lost or stolen card the total possible fraud amount would be low.

In countries like France and the UK where small amounts contactless transactions are authorized off-line, (meaning within the chip on the card and without the use of the processing network), the number of contactless transactions that can be made in a row with a contactless EMV card is limited. After a certain number of transactions, a reset with chip and PIN in contact mode is required or the card will automatically stop functioning in contactless mode.

One of the benefits of this contact reset is that it adds a regular verification process to check that the cardholder is truly the card owner.

When a contactless card is reported lost or stolen, the issuing bank will cover for the small amounts, if any, that a fraudster managed to spend before the security threshold.

In all other countries where transactions are authorized online (i.e. via the processing network), the PIN protects the cardholder in any large amount transactions. For small amounts where no PIN is required, contactless will stop working as soon as the cardholder reports his/her card stolen or lost.

The bank liability coverage will protect the cardholder in case any fraudulent small amount PIN-less transactions were performed prior to the card being reported lost.

THALES

> Thalesgroup.com <