INFORMATION SHEET

Skimming

How you can protect yourself

What is skimming?
Skimming is the illegal mining of client data during Maestro card or credit card data transactions.

How does skimming happen?
Skimming is when the data pertaining to your card are deciphered and saved by a manipulated reading device. A hidden mini camera also records you when entering your PIN code. This enables scammers to duplicate your card and withdraw cash using your PIN code.

How you can protect yourself from skimming?

- Double check that there are no conspicuous components (reading devices, mounted keypads, mini cameras, etc.) attached to the ATM. All ATM components are normally built very sturdily and cannot be removed.
- Do not let yourself get distracted during the transaction. Do not accept any help from people you don`t know.
- ATMs in a building are usually more secure. However, caution is always advised.
- Always use your free hand to cover the keypad while entering your PIN code.
- Check your monthly account statements.

What should I do if I notice a manipulated device?
Do not perform your transaction. Leave the ATM and immediately inform the police (tel. 117). If you have already used your card, contact your Bank CIC client advisor right away.

Outside normal business hours, please notify Telekurs AG on 044 271 22 30.

Your card will be blocked right away and thus can no longer be used by the scammer.

What should I do if money has been fraudulently withdrawn from my account?
Contact your Bank CIC client advisor without delay.

Your client advisor will be happy to answer any additional questions you may have.

Which devices are at risk of skimming?
Skimming can happen anywhere you use your Maestro card or credit card.

Skimming is possible at the following devices, among others:

- ATMs
- Ticket machines (e.g. SBB)
- Petrol stations

Important telephone numbers

- Bank CIC: 0800 242 124
- Telekurs AG: 044 271 22 30
- Police: 117

ZURNA20180323