Mozout

Generated on 14/11/2026 03:12

KNOWLEDGE BASE · PUBLIC DOCUMENT

What never to put in a transactional SMS: passwords, full card numbers and private details

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-7884	v2026.11.13	International · English

MozOut International
RLX Holdings (Pty) Ltd. · Group RLX Holdings
Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/7884

What never to put in a transactional SMS: passwords, full card numbers and private details

Security Created on **November 13, 2026** 3 min read



The short answer: in a transactional SMS, **never** include passwords, PINs, full card or account numbers, ID document numbers, health details or other private information. The SMS shows on the lock screen, stays stored on the phone, and the number may change hands. Give only enough for the customer to recognise the matter, and send the rest somewhere behind a password.

Why SMS is not a safe

1. **It shows on the lock screen.** Anyone nearby can read the preview without unlocking the phone.
2. **It stays stored.** The message sits on the phone until someone deletes it, and phones get lost, lent or sold.
3. **Numbers change hands.** A customer who stopped using a number may no longer be the one receiving it.
4. **Phones are shared.** In many families the same handset passes through several people.

Instead of this, write this

Instead of	Write
The new account password	«Your password was changed. Not you? Call [PHONE].»
The full card or account number	Only the last 4 digits: «account ***4521».
A medical test result	«Your results are ready. Please collect them at the clinic.»
The balance, when nobody asked for it	The operation and its amount; the balance is on your website or app.

Instead of	Write
The ID document number	The first name, if needed, and the case reference.

Verification codes are a different matter.
A code the customer asked for can go by SMS, with a short expiry and limited attempts: see **sending one-time codes safely**. What you never do is send a code or a password the customer did not ask for.

What the API already does for you

In API answers, the recipient's number comes **masked**, like `25884****567`, so it is not kept in full in your system's logs. Requests always travel over HTTPS, and each key can have an IP list. The message text is down to whoever writes it: whatever you put in arrives on the phone exactly as written.

Before a new text goes into your system

1. **Read it as if the phone belonged to someone else.** Would they learn something they should not?
2. **Remove whatever is not needed** for the customer to understand the matter.
3. **Swap the sensitive detail for a pointer:** «see your account on our website», «collect at the clinic», «call [PHONE]».

Guard your API key just as carefully.
Keep it in a vault or an environment variable, never in the code. If it leaks, follow **what to do when a key leaks**.

RECOMMENDED

Want useful notices that never expose your customers? See Transactional SMS.

See Transactional SMS →

SEE ALSO

- **Fake SMS in your company's name: helping customers recognise your real transactional messages** →
- **Writing transactional SMS: the key fact first, references and amounts, and one part only** →

Sending one-time codes (OTP) by SMS safely: expiry, attempt limits and logs

An API key or token has leaked: what to do, in the right order

Transaction alert SMS for banks, microfinance and payment services: what to include

SMS good practices and consent: who you may send to and how to let people opt out

Mozout

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-INT-KB-7884 · v2026.11.13 · Generated on 14/11/2026 03:12