Security Industry Insights for Finance

How to protect your bank from mobile fraud

5% of annual revenue

Lost due to fraud

Today's fraudsters are more connected and organized than they used to be. Their attacks are layered and more complicated. They've discovered ways to acquire larger payouts by attacking enterprises. Instead of seeking one-to-one targets, they seek one-to-many targets with complex, multifaceted schemes.

Mobile fraud continues to rise in 2023...

> For every $1 of losses to fraud, banks incur $4 in associated costs.
>
> —ABA Bank Journal, 2021

sopranodesign.com

soprano
communication unleashed

Security & Fraud Product Suite for Finance

IP Access Control

Allows admins to restrict access to IP addresses that are pre-approved. Login requests from any other IP address is denied, even if the login credentials are valid.

Single Sign On (SSO)

SSO integration gives organisations a centralised control system of access and reduces password fatigue for users which enhances the security.

2 Factor Authentication

2FA is the second layer of added security which a user can select to protect the account or system from attacks using stolen login credentials.

Finance Use Cases

IP Access Control

With more access breaches due to compromised logins and remote-work-friendly culture, financial institutions need to use additional measures to protect against malicious actors accessing their software tools.

Hi Susan. You are requesting a 2FA of your card ******9837. The code is 785410. Press 1 to repeat the message. Press 2 if you have not requested it. Press 3 if you want to speak to an agent.

Single Sign On

SSO is a foolproof way to reduce password fatigue when new security measures (like required password changes) are increasingly frequent.

2 Factor Authentication

Use 2FA to protect your messaging portal from bad actors who might use your verified number and portal to access your customers' accounts.

sopranodesign.com

Security & Fraud Product Suite for Finance

Simple Template Messaging

Admins can define standard templates to be used across an organization which creates brand consistency and added protection against undesirable messaging due to user error.

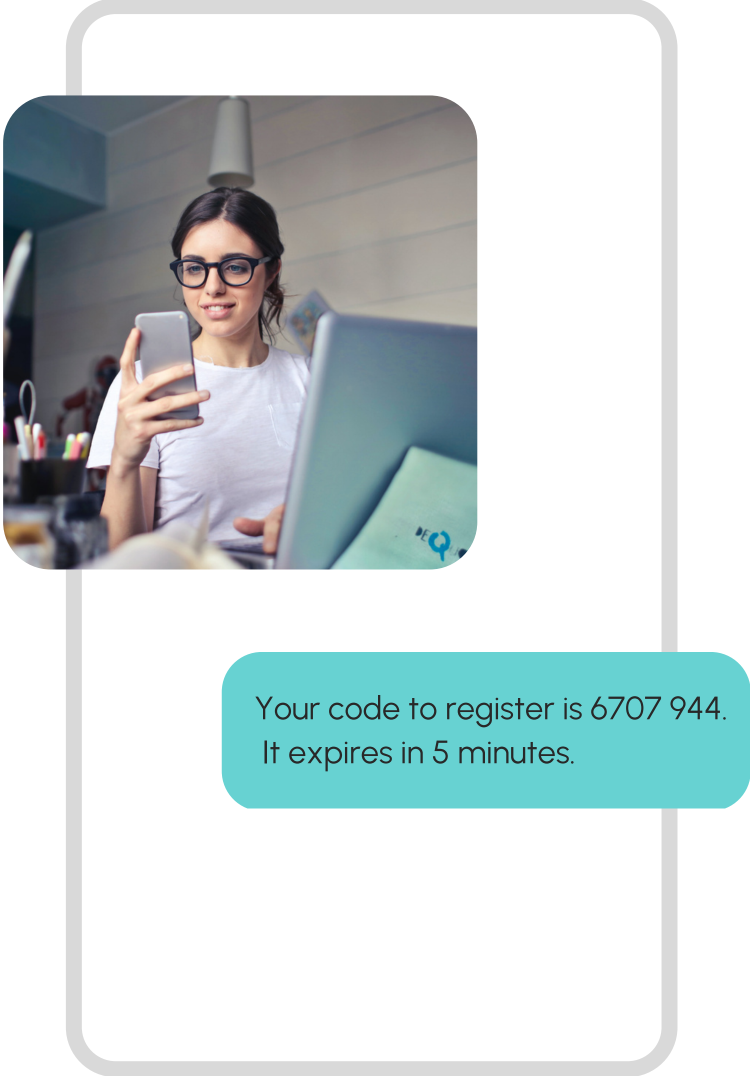
Authenticator

Enables secure access to online services via OTPs to authorize online virtual private network (VPN) access or financial transactions to reduce fraud and improve network security.

Approved List

This is the legacy filtering feature that allows users to employ standard opt-out/in management for all broadcast messages from the platform.

Finance Use Cases



Your code to register is 6707 944. It expires in 5 minutes.

Simple Template Messaging

Banks with multiple regions, branches, etc. will reply on STMs to create brand-consistent, compliant, and approved messaging for individual marketing and messaging teams to deploy as needed.

Authenticator

All financial institutions should use one-time passwords to secure logins of account holders for any portal. OTPs are also useful to secure individual transactions like security changes, transfers, and online withdrawals.

Approved Lists

All opt-in and opt-out choices made by your account holders over time need to be layered on to any new communication initiative—which necessitates the use of a legacy list.