

A low-angle shot of a woman with short brown hair, wearing a bright blue cape, looking upwards. She is positioned in the center-right of the frame. The background consists of tall, modern skyscrapers with glass and steel facades, reaching towards a bright, slightly overcast sky. The perspective creates a sense of height and aspiration.

8x8

Pumping the brakes on Artificially Inflated Traffic (AIT)

Protect against SMS Fraud with
8x8 Omni Shield

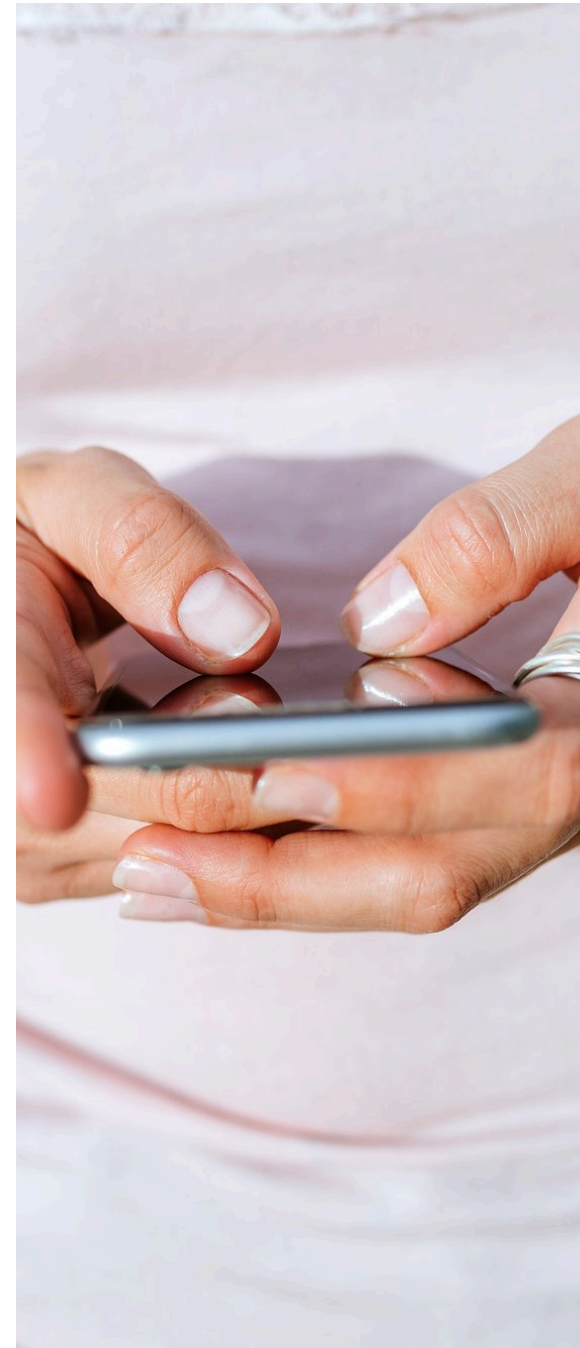
The escalating threat of
AIT in modern
telecommunications

When digitalisation presents both opportunities and challenges

[SMS remains one of the most popular and effective channels](#) for businesses to stay engaged with their consumer base, whether it's for marketing, customer service, or security purposes. But its immense global popularity has also made it a prime target for exploitation by cyber criminals and other rogue parties.

SMS pumping occurs when fraudsters trigger high volumes of text messages to be sent from unprotected SMS systems. They usually target automated channels like OTP requests, and then profit off the messages sent. Common marks include banking, e-commerce, social media, and ride-hailing apps, but any business can be vulnerable to SMS pumping.

Amongst the top threats of SMS messaging is Artificially Inflated Traffic (AIT), also known as SMS Traffic Pumping Fraud. Traffic pumping was [the second-most common telecom fraud](#) reported in 2021.



How does SMS pumping work?

Target Identification

Malicious actors identify vulnerable SMS systems, often those using automated channels like OTP requests.

SMS Volume Increases

They flood these systems with a large number of message requests, overwhelming the system.

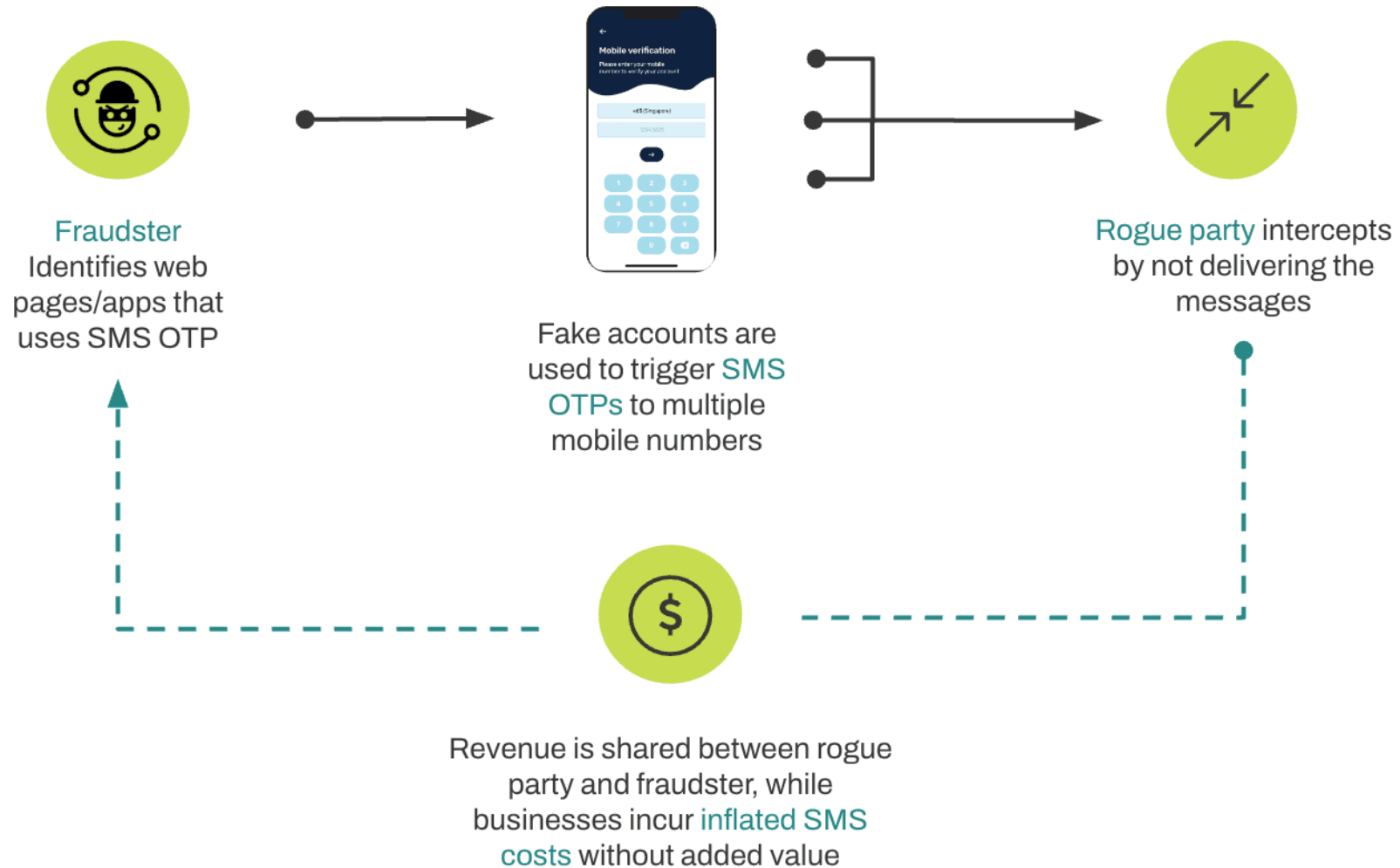
Profit Generation

By exploiting premium-rate numbers or receiving kickbacks, fraudsters profit from the increased SMS traffic.

Businesses Get Impacted

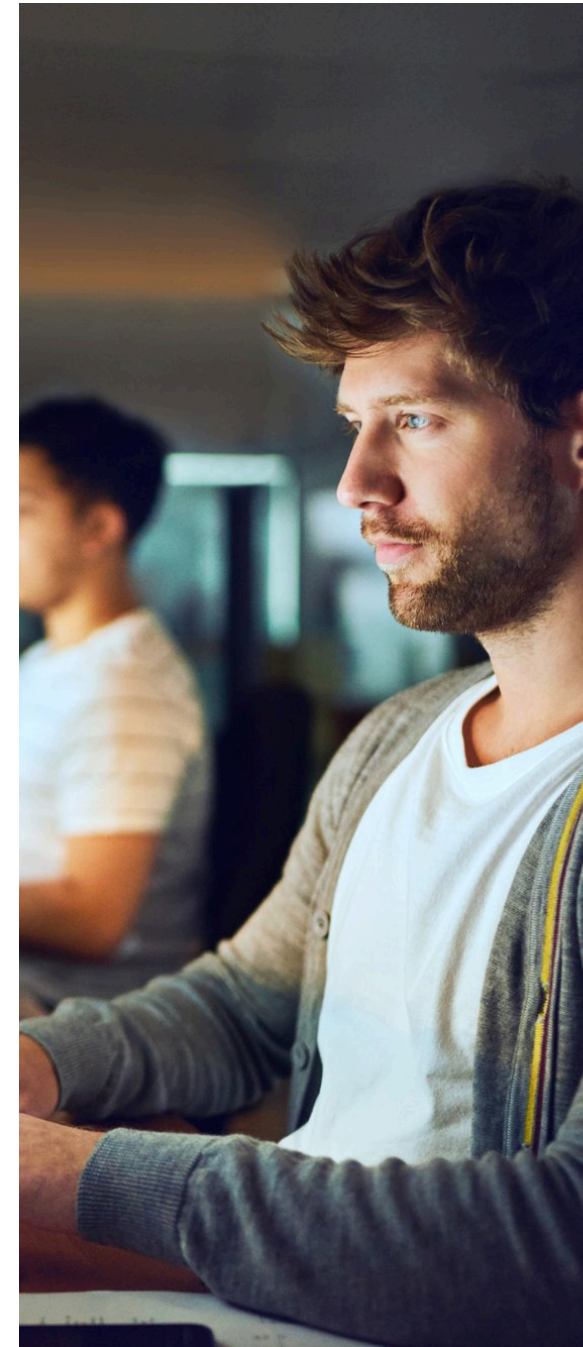
This fraudulent activity often leads to financial losses, damage to reputation, and operational disruptions for affected businesses.

How does SMS pumping work?



To catch SMS pumping before it escalates, watch out for some of the following symptoms:

- **Sudden spikes in incoming message volume**, especially if received during off-peak hours of your main target market, or from regions or countries that you don't normally get traffic from
- **Unexpected increases in SMS bills**, especially if you have no currently running marketing or promotional campaigns
- **Sequential number patterns** in the phone numbers sending you message requests, especially if clustered around the same timing
- **A discrepancy between engagement metrics and actual conversions**, suggesting inflated engagement from fake or non-genuine sources
- **Complaints from genuine customers** about difficulties reaching you due to network congestion



A woman with dark hair and glasses is shown in profile, looking intently at a computer monitor. Her hand is resting on her chin, suggesting deep thought or concentration. The background is a blurred office environment with other people working at desks. The lighting is soft, and the overall tone is professional and focused.

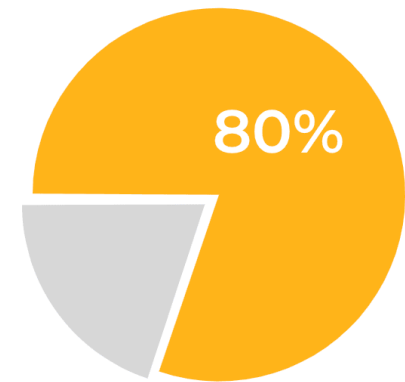
Understanding the toll
of AIT on your business

Don't become another statistic

AIT and SMS fraud affect businesses worldwide, across all industries. So yes, [your business is at risk too](#). And the consequences aren't just financial—customer experience also takes a hit, resulting in dissatisfaction and longer-term reputational damage.

**USD
\$6.7B**

Lost to SMS traffic pumping fraud, globally in 2021



As much as 80% of overall mobile traffic can be artificially generated traffic, i.e. SMS fraud

Sources: [Communications Fraud Control Association \(CFCA\)](#), [Infosecurity](#)



Financial costs

The most immediate consequence of SMS pumping is inflated messaging costs for these “empty” messages. These losses inflate if fraudsters use premium rate numbers, which incur significantly higher charges compared to standard rates.



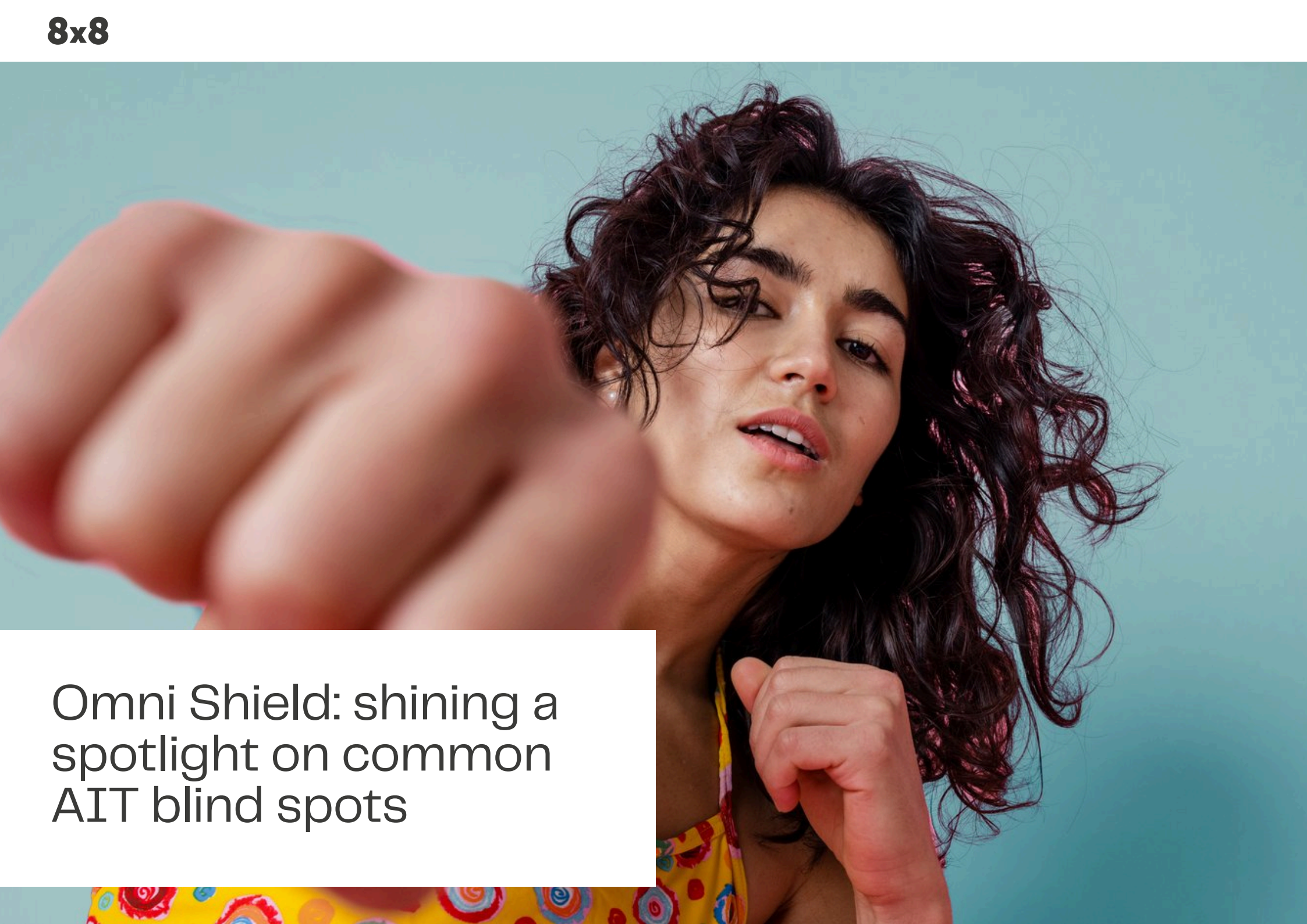
Resource drain

Even after fraud is detected, businesses still have to embark on the resource-intensive process of sifting through message reports, monitoring and blocking future fraudulent activity, and managing any service disruptions caused.



Operational disruptions

SMS pumping can disrupt normal business operations, causing delays in responding to genuine customer inquiries or requests. Customer complaints and damages to business credibility also require additional recovery effort.

A woman with dark, curly hair is looking over her shoulder towards the camera. A hand is in the foreground, out of focus, reaching towards the camera. The background is a solid teal color.

Omni Shield: shining a
spotlight on common
AIT blind spots

Why do some businesses fall prey?

Limited awareness of AIT and SMS traffic pumping is the main reason why businesses tend to fall prey to fraud. Most malicious actors also often target countries where customers do not operate in.

Research from 8x8 additionally found that amongst customers that have been targeted, 70% of them did not have a system for tracking their messaging/OTP conversions. This lack of insight resulted in them being unable to flag abnormal trends in time to act.

70% of customers encountering fraud did not track their conversion rate



Early detection and prevention of AIT with 8x8 Omni Shield

[8x8 Omni Shield](#) puts power back into the hands of businesses to protect themselves against SMS traffic pumping fraud. Not only can Omni Shield detect huge and abnormal spikes in messaging volumes, it is also capable of picking up slow, steady frauds through a combination of **traffic detection** and **phone number intelligence**.

Traffic Anomaly Detector

Analyse live traffic on abnormal trends using machine learning



Intelligently track suspicious change of Volume behavior based on your defined usage pattern



Track your conversion and delivery rates at the operator level based on your defined usage behavior



Monitor sudden changes in your operator breakdown or live traffic as indication of potential fraud

Phone Number Intelligence

Verify that a number is valid and responsive before sending an SMS



Profiling of number based on historical behavioural data to determine its risk score and activity status



Clean your database from unwanted corrupted data*

*You can do this with Phone Number Intelligence API, which will be launched soon

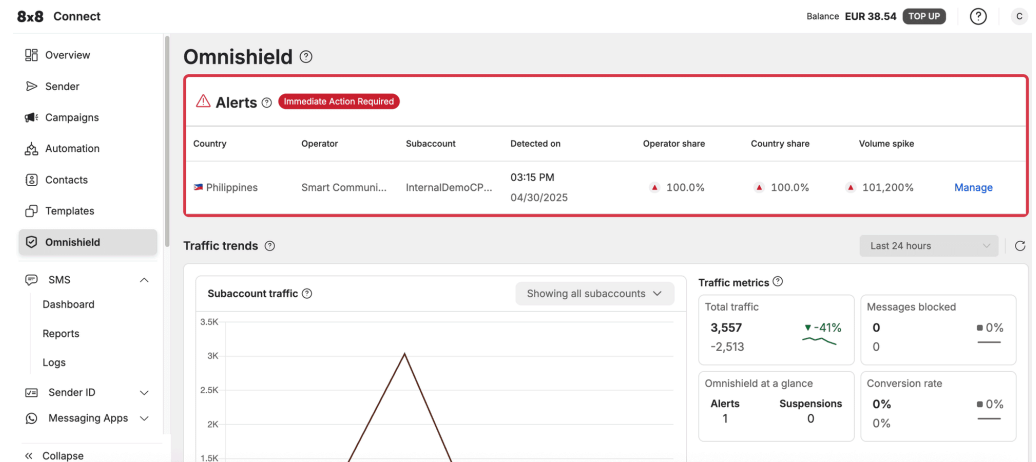
Make defence a seamless part of your SMS workflow

Future-proof your business against current and future threats by integrating fraud detection directly into your messaging workflow. 8x8 Omni Shield automatically detects and alerts suspicious behaviour so that you can take timely action as necessary.



Key features

- **Comprehensive metrics:** Gain real-time insights into traffic patterns, including total volume, conversion rates, country and operator ratios, blocked messages, and more. Detect unusual patterns early and stay ahead of potential fraud.
- **Rapid response:** When potential fraud is detected, you will be alerted immediately so you can choose to suspend operators or countries under attack, minimising risk and protecting your business.
- **Real-time alerts:** Receive instant notifications of suspicious traffic patterns, enabling you to log in immediately for a timely review and decisive action.



Immediate business benefits of 8x8 Omni Shield

Enhanced Security

Intelligent monitoring systems defend against AIT attacks by swiftly detecting anomalies and blocking suspicious activity. This bolsters security, safeguards your business, and boosts customer trust and confidence.

Cost Savings

Proactive measures to prevent AIT reduce the financial burden associated with fraud recovery, and preserve the integrity of your messaging channels, allowing you to focus more of your budget on legitimate communication efforts.

Real-Time Visibility

The ability to monitor messaging activity in real-time empowers businesses to swiftly detect and respond to AIT attacks, while additional insights on messaging patterns also safeguards your business against future fraudulent activities.

Optimise Conversion

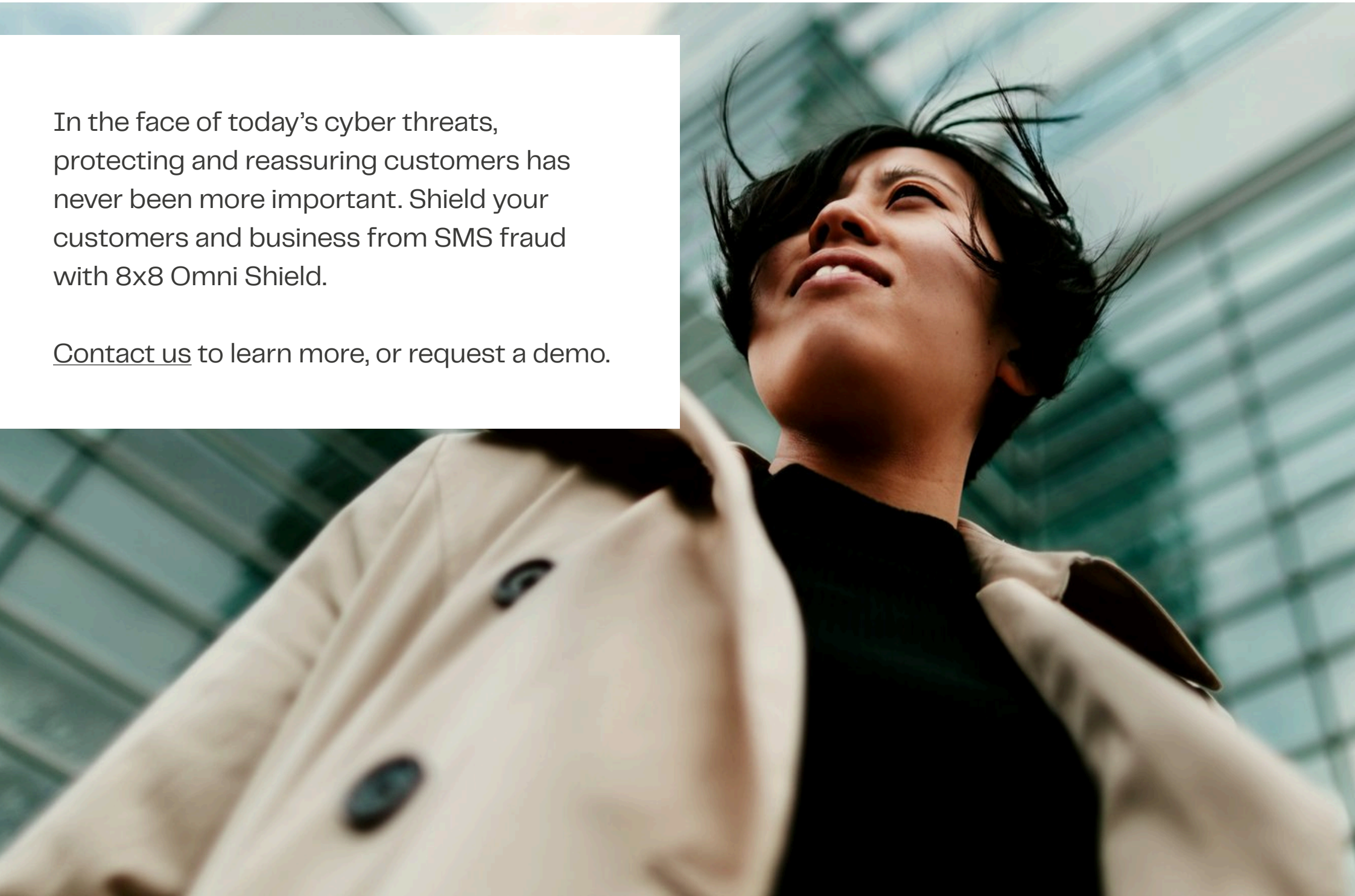
Maintaining an accurate and up-to-date customer database is essential for maximising deliverability and conversion. Removing outdated or inactive customer records allows businesses to optimise the impact of communication campaigns.

[Learn more about 8x8 Omni Shield for SMS Fraud Protection](#)

8x8

In the face of today's cyber threats, protecting and reassuring customers has never been more important. Shield your customers and business from SMS fraud with 8x8 Omni Shield.

[Contact us](#) to learn more, or request a demo.



Thank you for reading

Pumping the brakes on Artificially Inflated Traffic (AIT)

hello-cpaas@8x8.com

