



The network behind the world's top networks



THE GROWING THREAT OF CLOUD COMMS FRAUD AND HOW ENTERPRISES CAN ADDRESS THE RISK EFFECTIVELY

SUMMARY

The volume of international telecoms fraud has decreased in recent years, but its impact when successful is much greater. As new infrastructures such as the cloud join the telecoms spectrum, combatting fraud must be a priority for enterprises, to keep both customers and users safe, and to protect revenue. This white paper explores why the cloud has become an increasing target for various types of fraud and how service providers can proactively combat the threat.

CONTENTS

Introduction –
The rise and fall of
telecoms fraud



3

Why the cloud is the
perfect environment
for fraudsters to
target



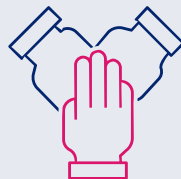
4

The biggest fraud
risks for cloud



6

A collaborated and
dedicated approach
is essential



7

Conclusion



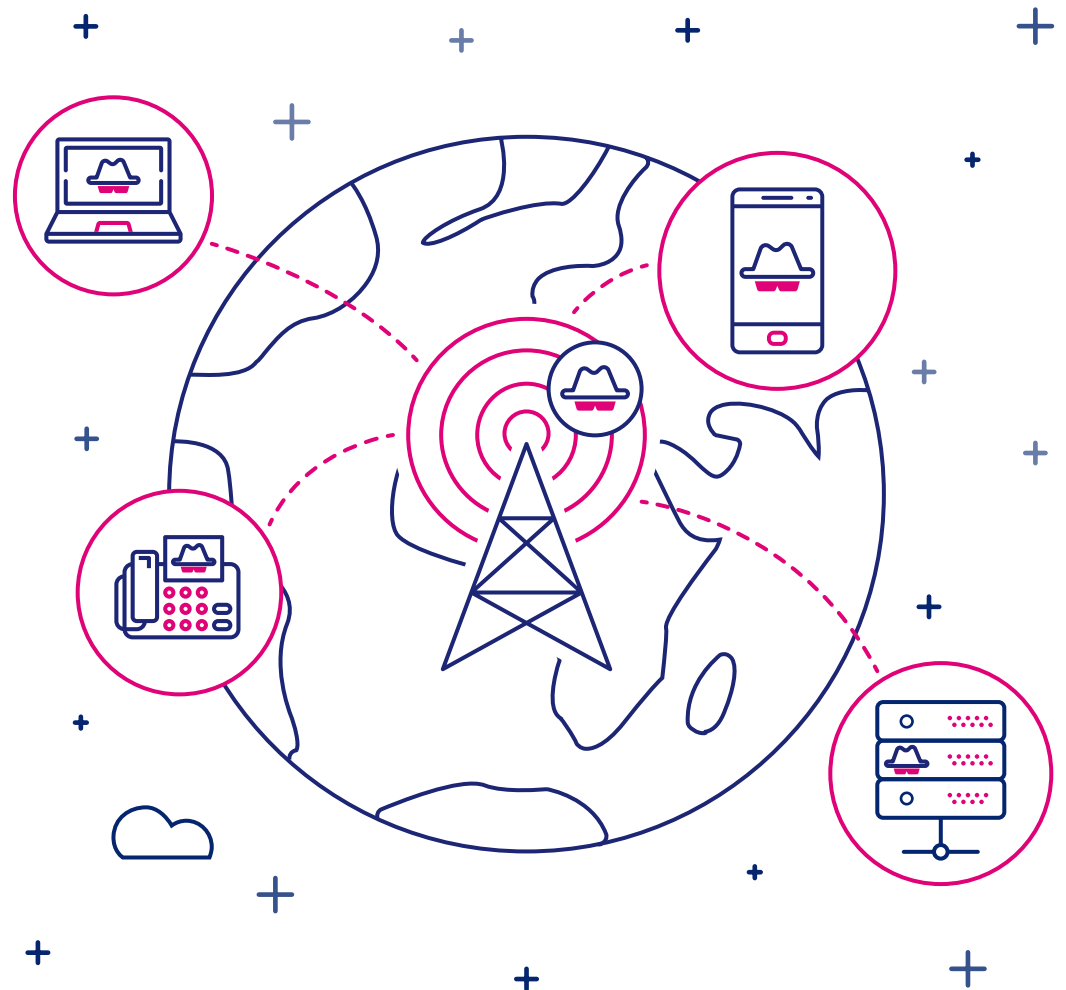
8

THE RISE AND FALL OF TELECOMS FRAUD

The international telecoms fraud environment is evolving. Criminals are increasingly operating on a global scale, running multinational organizations and finding new and sophisticated ways in which to commit fraud. In 2018, global telecoms fraud losses hit \$29.2 billion, with 66% targeting international traffic¹. Worldwide, the volume of fraudulent attacks across the telecoms industry seems in decline, down 5% from 2017 to 2018¹. However, the impact they now have on businesses is two-fold.

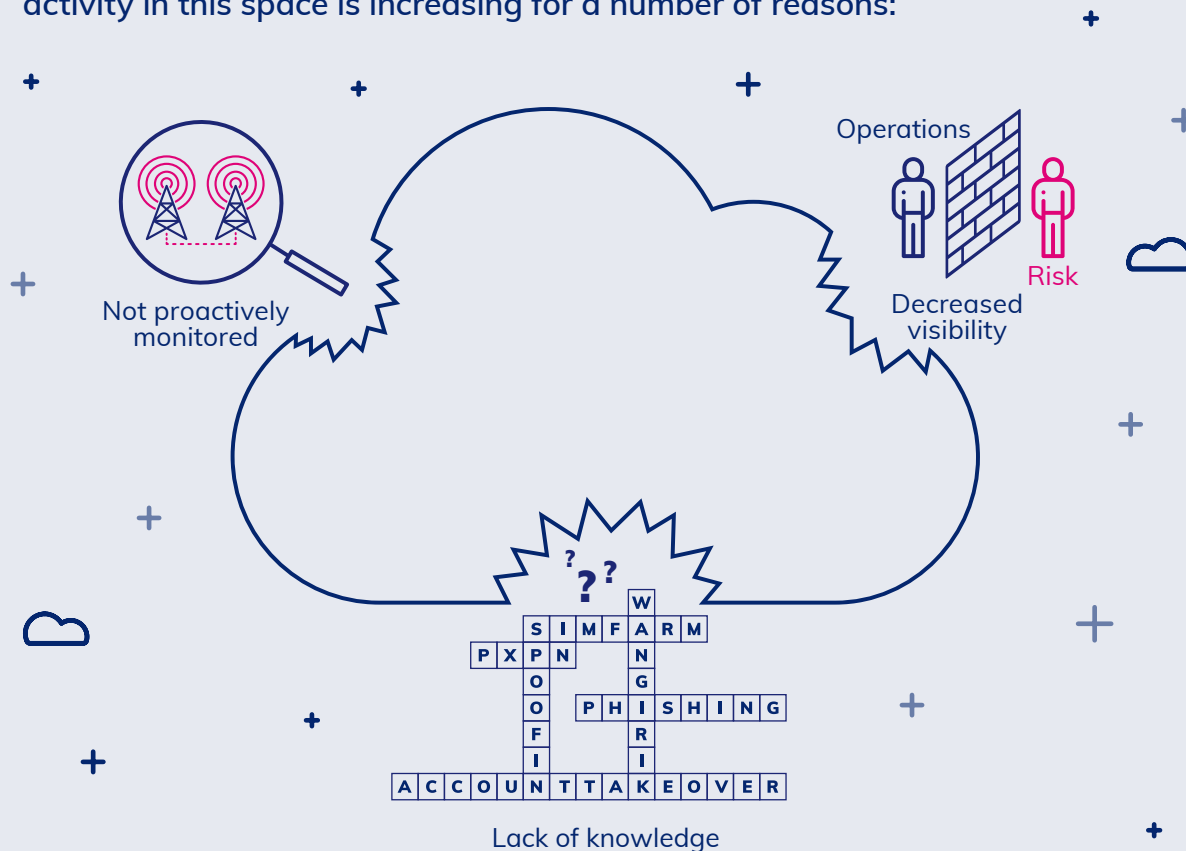
International traffic is becoming increasingly difficult to protect and secure. Country-specific regulations such as GDPR are barriers for many enterprises looking to adopt proactive security measures. The varying types and definitions of fraud across countries are another obstacle that businesses must maneuver, alongside cross-jurisdiction restrictions and sophisticated techniques that are making it increasingly difficult to actively catch criminals. Even when fraudulent activity is identified, the fraudsters themselves are usually long gone. But with new tactics must come innovative defenses.

¹ CFCA Fraud Loss Survey 2017



WHY THE CLOUD IS THE PERFECT ENVIRONMENT FOR FRAUDSTERS TO TARGET

Overall telecoms fraud may be decreasing, but younger segments within the industry are witnessing an increase in the volume and associated losses of fraud. Cloud communications is still relatively new when compared to more traditional telecoms, and its infancy is having a domino effect for contact centers and other providers of cloud services, such as numbers. Fraudulent activity in this space is increasing for a number of reasons:

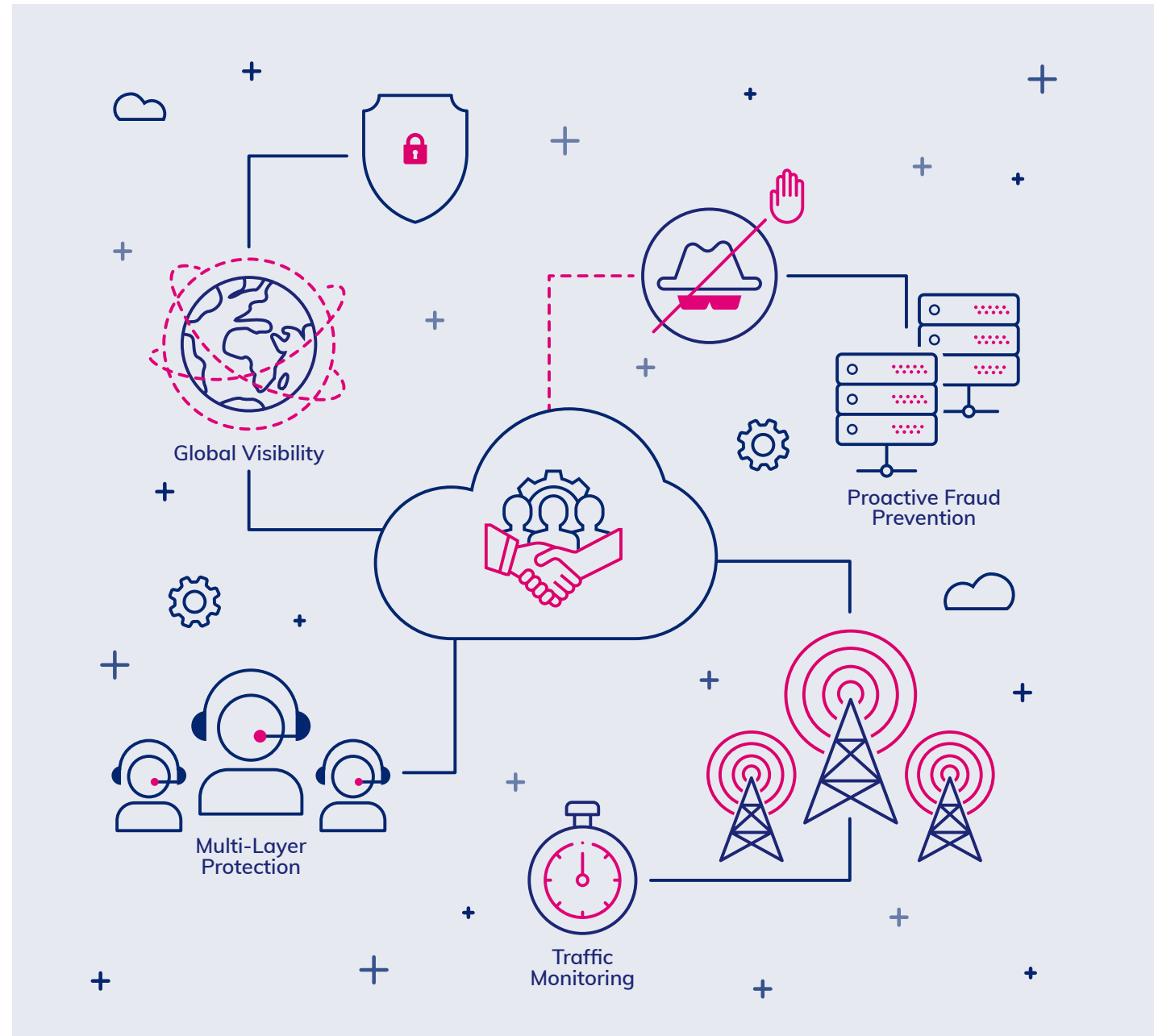


This combination offers up the cloud as the perfect environment in which fraudsters can operate.

Service providers offering cloud-based numbers are limited when it comes to the global historical data needed to proactively combat fraud. Although the different fraud types and methodologies are similar across the telecoms spectrum, service providers such as call centers need to utilize traditional telcos to combat fraud. With a backlog of relevant data points and fraudulent activity to draw upon, telcos are already well equipped to prevent fraud. This data translates to a wider knowledge of fraud, building on experience that has not yet had time to manifest for cloud infrastructure.

In addition, service providers need to have their cloud-based numbers monitored 24x7, to identify fraudulent activity before it can have devastating effects on the business. A lack of proactive fraud surveillance can allow fraudsters to take advantage of guarding loopholes, enabling them to target cloud numbers more easily. In turn, fraudulent activity can progress longer prior to being detected and ultimately, stopped.

Fraud detection can be made even easier with an end-to-end view of various teams and services within an organization. UcaaS and CPaaS providers for example often have a multi-layered work environment, involving complex ecosystems with workforces that are frequently geographically dispersed. Operating in silo can make it difficult to develop full visibility, which is needed to proactively detect fraud and stop it in its tracks. Ultimately, service providers also need to know where their cloud numbers are being utilized by the end user, to combat fraud more effectively internally. In order to gain visibility of where that number is being used once it has passed over to another area of the business or to the customer, an effective fraud solution needs implementing to provide a clear end-to-end view.



THE BIGGEST FRAUD RISKS FOR CLOUD

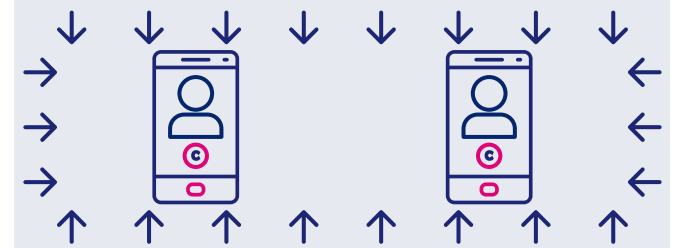
Recent statistics have shown a steady increase in fraud impacting new communications platforms, with 2018 demonstrating a 60% rise year-on-year, reaching a level where 32% of the fraud events pertain to Cloud Communications providers¹. Identity theft and fake account openings contribute significantly to these figures. Due to an overarching decrease in fraud awareness, the race for customer acquisitions – which can leave the door open to fraudsters – and a multi-layered business and customer ecosystem, these types of fraudulent attacks can remain undetected and unresolved for months at a time, resulting in thousands in revenue loss.

Cases relating to the misuse of communications services such as cloud-based numbers are also on the rise. Conferencing services utilizing cloud-based numbers can be exploited over long periods of time to enable large amounts of fraudulent traffic to be passed through. This often results in huge financial implications for the cloud communications provider.



Use case: Through proactively blocking 73776 calls, a leading UCAAS player saved more than €479,000 in fraudulent losses over a period of 8 weeks.

Use case: A conferencing services provider was hit by fraudsters misusing their global conference services for more than two months, transporting a massive amount of fraudulent traffic and causing a financial impact of \$480,000 USD.



A COLLABORATIVE AND DEDICATED APPROACH IS ESSENTIAL

Fraudsters are already taking advantage of the inexperience in fraud for businesses offering cloud-based numbers, such as UCaaS. Criminals are able to utilize more traditional and less complex technology and fraudulent methods to gain the best possible results with minimal effort. However, service providers can enlist the help of experienced and traditional telcos, to help proactively prevent telecoms fraud.

Collaboration is the key to fighting fraud in the cloud. By working with traditional telcos, service providers can tackle cloud number fraud more effectively. Drawing upon the wealth of knowledge and experience that operators have to hand from years' worth of familiarity and understanding, cloud numbers can be proactively protected from fraudsters. With vital around-the-clock monitoring and increased visibility, fraud is more likely to be stopped in its tracks.



CONCLUSION

With 25 years of experience in the telecoms sector, BICS has the knowledge and the experience that is key to help service providers in the cloud comms space to prevent fraud. The company's unique positioning and global multi-network view of quality of international traffic, makes it the ideal partner to proactively combat fraud. BICS' FraudGuard solution uses a collaborative crowdsourced platform that is constantly enriched and evolving through new data information, enabling simpler detection and proactive prevention of fraud. The solution's Intelligence Repository is populated with the details of more than 50 million known fraudulent numbers, collected across a partner base of more than 1,200 telcos. This enables pre-emptive blocking of known fraudulent numbers before they can impact service providers and their customers.

Knowledge and collaboration are key to preventing cloud number fraud. A secure solution that monitors numbers and provides full visibility is the answer to protecting service providers in the cloud against fraud.



The network behind the world's top networks

**FOR MORE INFORMATION ON HOW BICS
CAN ADD VALUE TO YOUR BUSINESS
CONTACT US AT WWW.BICS.COM**