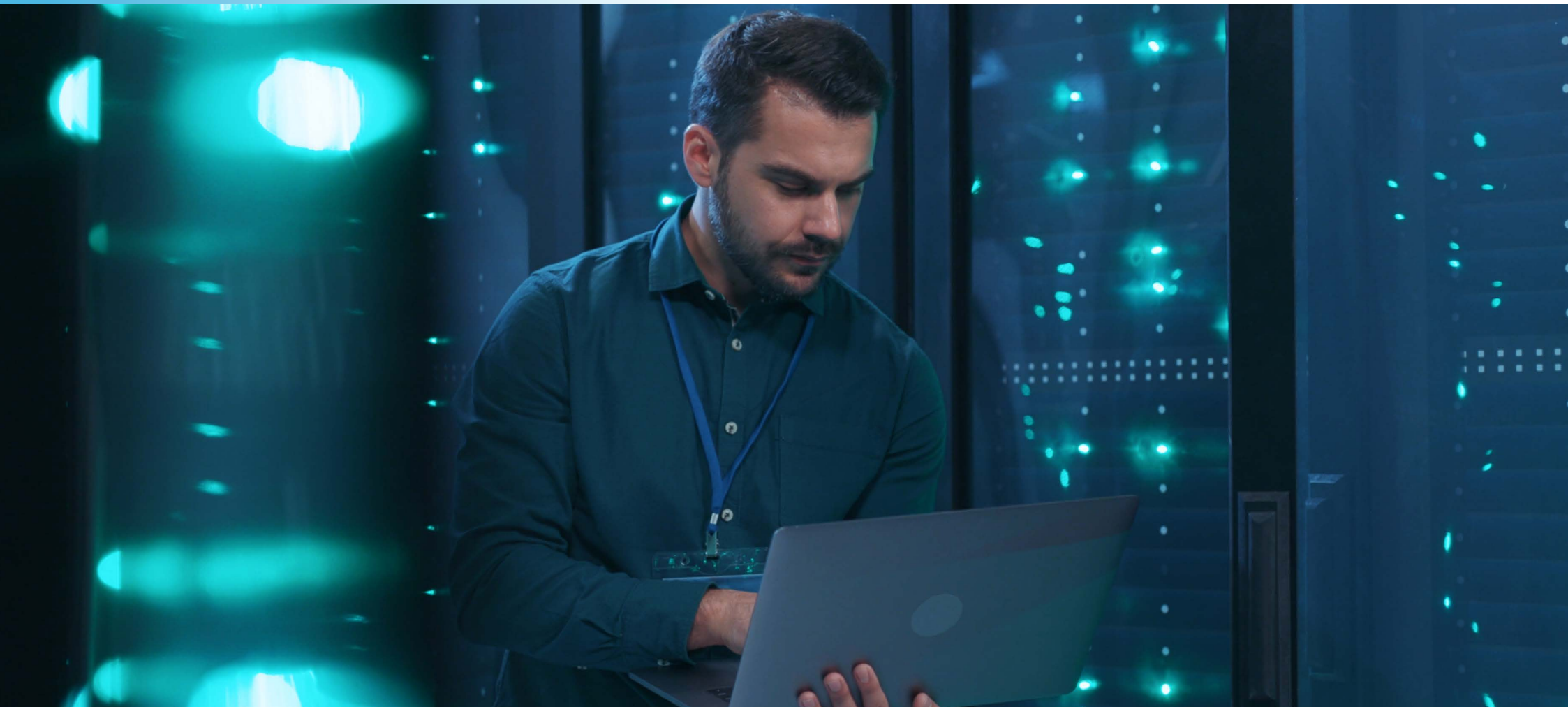
bics

The growing threat of cloud comms fraud and how enterprises can address the risk effectively



Summary

The volume and impact of international telecoms fraud is on the rise. As new infrastructures such as the cloud join the telecoms spectrum, combating fraud must be a priority to keep both customers and users safe, and to protect revenues. 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.

The rise 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 to commit fraud. In 2019, global telecoms fraud losses hit $28.3 billion, equating to 1.74% of revenue for telecoms operators. This compares to 1.27% of revenues in 2017, indicating that fraud loss and impact are on the rise[1].

International traffic in particular is becoming increasingly difficult to protect and secure. Country-specific regulations such as GDPR are barriers for many organizations 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. To fight these new tactics, innovative defenses are needed.

[1] CFCA Fraud Loss Survey 2019

Cloud communications needs telecoms expertise for fraud prevention

Newer segments are witnessing an increase in the volume of fraud and the losses associated with it. Cloud communications is still relatively new when compared to more traditional telecoms, and its infancy is having a domino effect for contact centers and providers of cloud services.

Fraudulent activity in this space is increasing for a number of reasons:

- Lack of knowledge
- No proactive monitoring
- Decreased visibility

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. As a result, service providers such as call centers need to utilize traditional telecoms providers. With a backlog of relevant data points and fraudulent activity to draw upon, they 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 take place for longer before it is 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 dispersed geographically. Operating in silos can make it difficult to develop the full visibility 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 if they are to combat fraud 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

There is a steady increase in fraud impacting new communications platforms. Identity theft and fake account openings contribute significantly to this trend. Due to low 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 revenue losses of hundreds of thousands.

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 to enable large amounts of fraudulent traffic to be passed through. This often results in huge financial implications for the cloud communications provider.

By proactively blocking 73,776 calls, a leading UCaaS player saved more than €479,000 in fraudulent losses over eight weeks.

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

A collaborative and dedicated approach is essential

Fraudsters are already taking advantage of the inexperience of fraud that businesses offering cloud-based numbers can have. Criminals are able to utilize more traditional, less complex technology and fraudulent methods to inflict the most damage with minimal effort. However, service providers can enlist the help of experienced telecoms providers to proactively prevent telecoms fraud.

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

Conclusion

With 25 years of experience in the telecoms sector, BICS has the knowledge that is key to helping service providers in the cloud comms space prevent fraud. The company's unique positioning and global multi-network view of international traffic quality, makes it the ideal partner to proactively combat fraud. BICS' FraudGuard solution uses a collaborative crowdsourced platform that is constantly enriched and evolving with new data, 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.

For more information, visit at www.bics.com

For more information, please visit:
www.bics.com