GlobalData.

Wholesale Antifraud: Competitive Landscape Assessment

Stradling, Joel

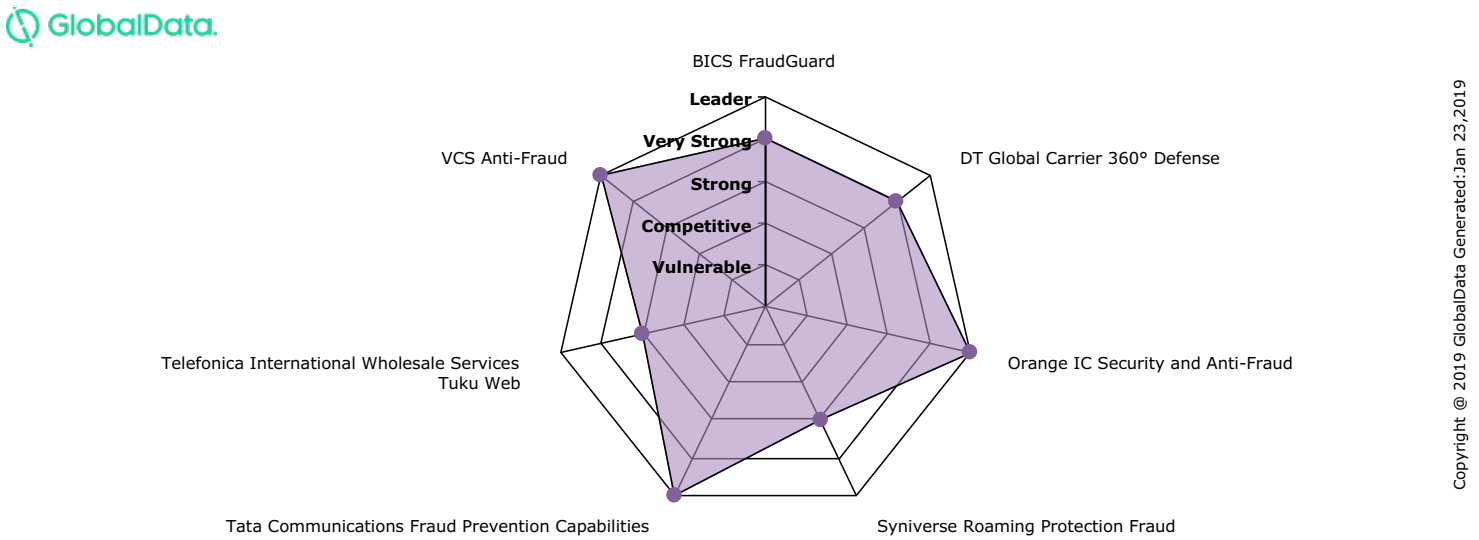
January 23, 2019

COMPETITIVE LANDSCAPE ASSESSMENT - WHOLESALE ANTI-FRAUD

REPORT SUMMARY

This report analyzes the competitive landscape for wholesale antifraud services. Operators offer constantly evolving antifraud capabilities for voice, data connectivity, SMS, roaming, signaling, and A2P messaging.

PRODUCT CLASS SCORECARD



MARKET OVERVIEW

Product Class	Wholesale Antifraud
Market Definition	Wholesale antifraud covers security solutions offered by major wholesale telecommunications providers to their partners, channels, and customers. In addition to traditional network security and voice fraud protection (DDoS protection, encryption, intrusion detection, firewall, anti-malware, anti-phishing, etc.), this segment is rapidly evolving to offer more sophisticated levels of protection, including protecting mobile traffic with SMS firewalls; business intelligence; traffic monitoring for anomalies; monitoring numbers, plans, and allocations; isolation of grey routes; setting rules, alerts, and traffic pattern thresholds; and overall fraud management. Competing service providers also offer expert support teams with experience, training, and expertise in combating fraud, with services extended to clients as advisory/consulting.
Rated Competitors	• BICS • DT Global Carrier • Orange International Carriers • Telefonica International Wholesale Services • Vodafone Carrier Services • Syniverse • Tata Communications

Additional Competitors	• iBasis (a Tofane Global Company) • BT • AT&T • Verizon Partner Solutions • Telia Carrier • TI Sparkle
Changes Since Last Update	• "BICS Expands MNO Value Proposition with New Local SMS Firewall Service Launch," August 08, 2018

MARKET ASSESSMENT

Types of fraud are diversifying as the attack landscape widens. This is creating a bigger demand for products and services from carriers. Service providers are responding by developing tools to support antifraud services, including highlighting dedicated expertise and support teams, as well as developing innovative capabilities, such as applying ML/AI to improve response. Carriers view antifraud as a value-add that can increase customer loyalty, help customers increase revenues, and improve quality of service. Market leaders are emerging, including for example Tata Communications, Orange IC, Syniverse, VCS, and BICS. The future of antifraud will be increasingly automated and intelligent as industry focus widens to secure technologies for 5G and connected things. Insight into traffic patterns and sophistication in applying business intelligence is opening new revenue streams for MNOs. There have been a number of fraud protection announcements in the previous several months, especially around SMS messaging and roaming SS7 fraud protection. Examples include BICS FraudGuard and DT Global Carrier's SMS firewall.

MARKET DRIVERS

• **Fraud Criminal Sophistication:** Attacks on service provider networks are carried out by very sophisticated criminal gangs. Customers of wholesale voice, data, and mobile signaling must turn to skilled and experienced wholesale providers to protect their revenues and reputations. Attacks are becoming more frequent largely on IP networks. The emergence of IoT gives fraudsters more points at which to make ingress into a network.

• **Agreement and Cooperation:** Service providers are working closely with partners and competitors in order to jointly battle fraudsters. Carriers, for example, continually update and share grey number listings to help close those lines down to prevent fraud.

• **Multiple Layers of Security and Harnessing AI:** The strongest protections against fraud come from multiple layers of security, such as firewalls, encryption, DDoS protection, and intrusion detection. Robots and AI are beginning to appear to make antifraud systems more automated and powerful.

BUYING CRITERIA

• **Portfolio:** Customers seek protection for multiple areas of their voice and data businesses. Voice is currently the largest fraud business in terms of revenue losses. MNOs also seek antifraud components for SMS, signaling, and roaming services.

• **Support:** Customers want to see proven credentials and have access to expertise. Most operators have a dedicated antifraud unit that will support customers and provide advice and guidance as well as training on tools and secure practice.

• **Service Management:** Customers appreciate the choice of self-managing the antifraud services – for example, setting thresholds on traffic and when to block – as well as the option to fully outsource the antifraud capability, giving management and control over to the carrier. Management tools and antifraud-as-a-service will be examined by prospects.

• **Partnerships:** Few operators approach fraud protection alone. The industry accepts that cooperation between providers and participation in independent industry bodies such as the i3 Forum are important to build the best levels of protection.

• **Innovation:** Advancements in machine learning and AI, and more intelligent networks, are giving rise to predictive fraud, intelligent fraud, and more proactive fraud response – for example, reacting to block a route before the fraud takes place based on anomalies.

VENDOR RECOMMENDATIONS

• **AI and Data Analytics on the Roadmap:** Operators have opportunities to achieve differentiation in a crowded landscape by developing antifraud capabilities that are more real-time and faster in response. Applying machine learning algorithms to data analytics on voice networks and offering clients innovative solutions may go a long way to scoring unique selling points.

• **Partnerships:** Operators that do not have robust antifraud capabilities may need to shore up their security and antifraud policies. The industry is more transparent thanks to new antifraud and monitoring capabilities, and most operators know which carriers may be taking part in less honest practices. The operators covered in the competitive landscape assessment may be able to assist since many offer advisory services.

• **Multilayer Security and Narrowing Exposed Surfaces:** Operators should aim to combine fixed and mobile network security such as IPX security, encryption, anti-DDoS, roaming protection, SMS firewall, and sharing A and B lists. Reducing the ingress into the network of criminals via multiple endpoints will be increasingly important as IoT adoption grows.

BUYER RECOMMENDATIONS

• **Choice in the Market:** There are currently many options available to wholesale and retail telecommunications providers to shore up revenues based on antifraud solutions. Customers are encouraged to ask voice, mobile messaging, and data suppliers for discussions that revolve around looking at the existing platforms, performing vulnerability audits, and soliciting recommendations on how antifraud services may help to grow revenue streams and strengthen service quality.

• **Self-Enablement Tools and Portals:** Service providers are extending sophisticated self-manage options to customers, as well as more real-time monitoring portals and interfaces. Clients should talk with suppliers to see how they might be able to take advantage of such options to be able to gain back some control over their voice, mobile, and messaging systems. Conversely, some operators are willing to take over full management of the antifraud solutions.

• **Voice Antifraud Basics:** For entry-level voice antifraud, a standard minimum level of protection should include regularly updated (e.g., daily) number lists, A and B numbers, details on grey routes, filtering, and the setting of thresholds and blocking rules. Providers should also be offering 24/7 monitoring and support services, with access to a team of experts or analysts to help advise on building robust antifraud.

ADDITIONAL RATED COMPETITORS

Product Name	BICS FraudGuard
Buying Criteria Rating	• Portfolio: Very Strong • Support: Leader • Service Management: Very Strong • Partnerships: Very Strong • Innovation: Leader
Product Scores	Very Strong
Strengths	• BICS has a major global voice business and can see at a global scale when fraud is taking place. • BICS offers a fully managed antifraud suite and is testing ML and AI solutions. • BICS developed its own platforms, and it runs them in the cloud. A shareholde is MTN; this gives advantages in the Africa/Middle East regions that are prone t fraud activities – in particular, SIM box bypass.
Limitations	• VCS and Tata Communications carry large voice traffic volumes and have developed compelling antifraud capabilities. Therefore, the competitive landscape is crowded. • Operating a large quantity of interconnections with other carriers can make it more difficult for BICS to protect traffic on portions of network that it cannot control. VCS reports 120 interconnections, and the shorter 'call-chain' means tighter fraud protection. • VCS can leverage its opcos to enforce antifraud policies.

Product Name	DT Global Carrier 360° Defense
Buying Criteria Rating	• Portfolio: Very Strong • Support: Leader • Service Management: Very Strong • Partnerships: Very Strong • Innovation: Leader

Product Scores	Very Strong
Strengths	• DT operates a 24/7 fully automated near real-time big data monitoring and blocking solution (A- and B-numbers) for all international voice traffic within the network. The solution can also identify and stop Wangiri attacks. Its big data solution is being used to develop a ML-based capability. • Dedicated seven-strong antifraud team plus part of the large DT Group. DT Global Carrier can offer customized solutions and support. • Comprehensive 360° defense strategy comprising: voice protection, SS7 firewall, SMS protection, MPLS-based IP VPN, global IPX, 'fraud-fighting' voice and SMS+, and volumetric and application-based DDoS protection.
Limitations	• In a crowded competitive landscape, DT Global Carrier may find it difficult to differentiate, since many operators offer fairly similar antifraud capabilities. • Mature competitors include Tata Communications, VCS, Orange IC, and BICS. • DT Global Carrier may need to bulk up the staffing of its antifraud team and deliver wider geographical coverage.

Product Name	Orange IC Security and Anti-Fraud
Buying Criteria Rating	• Portfolio: Leader • Support: Very Strong • Service Management: Very Strong • Partnerships: Strong • Innovation: Very Strong
Product Scores	Leader
Strengths	• Orange IC offers a very comprehensive cybersecurity range for networks including threat tracking, ID protection, and network audit and protection. Solutions are backed up by a dedicated 24/7 fraud protection team. • Orange IC can leverage the Orange Group's Cyber Defense team and facilities to strengthen global security. Machine learning is being applied to antifraud protection within the Cyber Defense organization. • Tailored and standard offers for interconnect roaming and margin protection. The components include bypass detection, QoS and revenue assurance, and financial transaction security. • SMS Fraud Detection tool detects intrusive SMS fraud via periodic audits, to identify existing fraudulent activities such as SIM box fraud and bypass. • Fraud and revenue assurance experts perform analysis. Orange IC offers managed services to support MNOs with grey-route detection, rules management, reporting, and market analytics on for the A2P market. • Orange Call Tracking System (CTS) runs automated and massive testing via more than 1 million calls per month on 1,000+ operators and routes to detect fraudulent SIM boxes.
Limitations	• The Orange Group has several subsidiaries in Africa and the Middle East, and these regions are known to be hotbeds for criminal fraud activities, exposing the carrier's network to attacks.

Product Name	Syniverse Roaming Protection Fraud
Buying Criteria Rating	• Portfolio: Strong • Support: Strong

	• Service Management: Strong • Partnerships: Strong • Innovation: Strong
Product Scores	Strong
Strengths	• Syniverse offers 24/7 support including a hotline, a portal, and access to a team of antifraud analysts. • Scale: 120 operators deployed Syniverse defenses globally; the system detects millions of dollars of fraud annually. Centralized global data patterns are leveraged to help identify fraud attempts in real time. • Roaming fraud specialist, with a solution that combines intelligent data capabilities with human analysts.
Limitations	• A number of large global telecommunications incumbent operators have considerable depth in their security and antifraud offerings, also covering, for example, fixed network anti-DDoS, such as Orange IC and DT Global Carrier. • Operators that provide on-net service to mobile subsidiaries, such as VCS, can leverage internal customer bases for scale and a first foot in the door for sales. • Most competitors also offer 24/7 monitoring and near-real time response to fraud activities; therefore, differentiation is a challenge.

Product Name	Tata Communications Fraud Prevention Capabilities
Buying Criteria Rating	• Portfolio: Very Strong • Support: Very Strong • Service Management: Very Strong • Partnerships: Very Strong • Innovation: Leader
Product Scores	Leader
Strengths	• Tata Communications runs a dedicated 'tiger' team for combatting fraud on behalf of its customers. • A major-scale voice business and strong cooperation and partnerships with other Tier 1 players give the company a strong position to see what is happening in its voice platform. • Tata Communications has developed a range of powerful capabilities to protect its customers against fraud, and it is pushing innovation with new tools in development.
Limitations	• Unlike VCS and Orange IC, Tata Communications does not have on-net information on a vast number of internal mobile subscribers.

Product Name	Telefonica International Wholesale Services Tuku Web
Buying Criteria Rating	• Portfolio: Strong • Support: Strong • Service Management: Strong • Partnerships: Very Strong • Innovation: Strong
Product Scores	Strong
Strengths	• The wholesale division is protecting the Telefonica Group worldwide from

	fraud incidents with a dedicated team and 24x7 support. • Big data analytics is being deployed in its antifraud solution, and there are developments underway to support AI for more sophisticated antifraud. • Telefonica International Wholesale Services serves the local Telefonica operating business from the same platform. • The company is an active member of the i3 Forum Antifraud Working Group and GLF, and it supports the 'Code of Conduct' global carrier antifraud initiative. • Scale: TIWS is managing more than 2 billion voice minutes per year internationally. • The Tuku IN solution generates more than 60k calls/month, reaching 100k calls/month to detect frauds. Telefonica can conduct testing with more than 25(carriers. • Telefonica operates according to strict antifraud policies and extends support tools to its customers. • The international scale and reach of Telefonica's global voice business means that the carrier can see fraud incidents on a global scale, and this experience and scale strengthen its antifraud practice and proposition.
Limitations	• More could be done to communicate the future roadmap in terms of predictive response to antifraud – backed up by big data analytics and ML/AI. • Telefonica's antifraud portfolio is very similar to those of its peers, making differentiation a challenge.

Product Name	VCS Anti-Fraud
Buying Criteria Rating	• Portfolio: Very Strong • Support: Leader • Service Management: Very Strong • Partnerships: Very Strong • Innovation: Leader
Product Scores	Leader
Strengths	• VCS can leverage its opcos to enforce antifraud policies; the operator manages 2.5 billion minutes per month on behalf of both Vodafone Group subscribers and wholesale traffic partners. • Fewer interconnections – approximately 120 – mean shorter call chains and higher levels of security. • VCS offers layers of defense, starting with firm control on the network and good knowledge of its suppliers for managing number plans daily and extensive SMS messaging firewall and security capabilities. • VCS has a unique differentiator in that it cooperates with law enforcement including Europol and the Law Enforcement Agency (LEA) to help identify criminals.
Limitations	• Some operators may suggest that having 1,000 or more interconnections gives greater information input regarding fraud activities. • There is room for disruption as players seek to leverage ML/AI to develop predictive and proactive real-time response.

GlobalData PLC,
John Carpenter House,
7 Carmelite Street,
London,
EC4Y 0AN,
+44 (0) 207 936 6400