TARGETOO

Transparency and Brand Safe Advertising

TARGETOO

Index

1. Executive Summary

1.1. Targetoo Mission

Targetoo is excited to introduce this whitepaper. Our goal is to enlighten businesses about the digital landscape's potential, particularly focusing on the rise of Direct Carrier Billing (DCB).

Targetoo aims to attract customers to your online platform by employing advanced User Acquisition strategies for Mobile Subscription Services.

As the customer journey unfolds, Targetoo steps in to fortify the anti-fraud efforts. Targetoo devises innovative solutions not just for identifying fraudulent activities but also for shielding against them. The primary goal of the company is to empower firms in the mVAS realm to cultivate enduring revenue streams from DCB through comprehensive market insights and protective measures. These measures encompass safeguarding both customers and businesses from ad fraud and payment page fraud, while also mitigating the financial fallout of non-compliance.

1.2. The Challenge

In the modern digital landscape, fraud is widespread and intricate, making it challenging to handle on your own. Marketing fraud tactics such as click spam, click injection, and SDK spoofing aim to boost impressions, clicks, and installations. Additionally, non-compliant practices like deceptive content can harm brand reputation and lead to complaints. These activities not only disrupt acquisition campaigns but also drain marketing budgets, costing companies both time and money.

When customers start using a company's services, fraud attacks on the company can also harm the customers' personal finances significantly. Fraudulent activities can result in unauthorized purchases, the exposure of personal data, and potentially even access to personal banking information.

1.3. The Solution

The key is to implement anti-fraud measures to safeguard the business's advertising practices and enhance the customer journey for its consumers. Targetoo provides the necessary solutions for businesses to implement effective anti-fraud practices.

One effective anti-fraud measure to consider is Direct Carrier Billing (DCB), a secure payment method. In this approach, customers make online purchases that are billed through their mobile carriers and then forwarded to them. DCB is a rising trend that offers numerous advantages for companies, particularly in areas like Europe, MENA, Africa, and Asia.

Though DCB carries certain fraud risks, companies can mitigate these risks by engaging cybersecurity and compliance professionals. These experts assist in establishing preventive measures against fraudulent activities. Moreover, in case of any incidents, the team can promptly address and resolve the issue, safeguarding both the company and its customers.

1.4. A Synopsis of the Whitepaper

In this whitepaper, you will delve into the evolving landscape of fraud impacting the digital realm. Discover prevalent fraud tactics and explore effective solutions to tackle these challenges.

As DCB is an emerging payment process to counteract fraud for consumers and reduce barriers for individuals making online payments, this whitepaper is focussed on what DCB is, why it benefits businesses, and the countries ideally positioned for brands to penetrate the market with DCB payment options. Through a regional analysis, we'll dive deep into what challenges exist in each region and the regulations in place to protect companies that operate there, and their customers.

2. DCB Industry Landscape

2.1. Market Overview

Mobile users prefer convenient and secure payment options, explaining the rise of Direct Carrier Billing (DCB) as a favored method in the past decade. Surpassing traditional methods like credit/debit cards and e-wallets, DCB offers a secure payment solution without the need to disclose financial details. With DCB, users can easily pay by having charges added to their mobile phone bills. During checkout, users input their mobile number and confirm the payment, providing an added layer of security. It's no surprise that DCB is projected to account for 11% of all digital payments by 2025. According to research, the global DCB market was valued at approximately USD 23.5 billion in 2019 and is forecasted to reach around USD 172.8 billion by 2027, with a Compound Annual Growth Rate (CAGR) of about 29.7% between 2020 and 2027.

DCB Benefits

The primary advantage of DCB lies in its secure interface. In the digital age we live in, cybercriminals and fraudsters are constantly active. Therefore, it is safer to utilize your mobile bill for payments rather than storing personal financial information. Moreover, the security measures extend with anti-fraud solutions. In section 3.2 of this whitepaper, we will explore the anti-fraud initiatives aimed at establishing DCB as a top option for secure transactions.

The advantages of DCB extend to its inclusive nature. With 1.4 billion people lacking a traditional bank account, DCB eliminates this obstacle, enabling these consumers to shop online. This is particularly crucial in regions where obtaining a bank account is difficult. In Iraq, for instance, individuals are five times more likely to own a mobile phone than have a bank account.

The simplicity of DCB is also a valued benefit. Consumers won’t need to search

For credit card users or those dealing with intricate online payment systems, a smooth online process results in more transactions and improved conversions for retailers, ultimately benefiting them. As retailers see an increase in their profits, mobile carriers also benefit. Direct Carrier Billing (DCB) frequently results in commissions being paid by the merchants.

Growing DCB Adoption

Consumer perceptions of Direct Carrier Billing (DCB) are on the rise as it becomes more mainstream and widely recognized. According to data from the Mobile Ecosystem Forum, there was a 2% increase in positive perception from 2022 to 2023 regarding the speed, convenience, and safety of DCB. This surge in positive perception has led to 42% of consumers acknowledging its convenience.

But as this payment method gains wider acceptance, the digital landscape has broadened to encompass physical products and services as well. Notably, ticketing has emerged as the most rapidly growing sector, experiencing a remarkable expansion of over 200% from 2023 to 2027.

DCB usage is evolving and expanding geographically. Currently, Europe holds the largest share of the global e-publishing market through DCB at 45%. As mobile phones are the primary devices for DCB, there are significant opportunities worldwide, especially with the expansion of the 5G network. India and MEA are rapidly growing in this sector, with a 37.7% and 37.3% CAGR of Carrier Billing spending respectively, and an expected 803 million users by 2027. Latin America is also catching up, with a projected CAGR of 25.1%.

How It Works

The DCB consumer process is very straightforward. These five steps indicate the ordinary course of action:

1. The user decides to make an online purchase and sees “Pay by Phone” as a payment option.
2. The merchant’s carrier billing provider transmits the order to the consumer’s contracted mobile network provider.
3. The consumer already has a registered mobile phone number or SIM card with an agreement for pre-paid or postpaid account transactions. Therefore, the mobile network provider simply verifies the user and confirms the funds so the purchase can be completed with the merchant.

4. The consumer's mobile network provider will then collect the funds. For a pre-paid account, funds can simply be deducted. For a postpaid account, the charge will be added to the upcoming monthly phone bill.
5. The mobile network provider then pays the merchant the total amount within an agreed-upon and specified period of time.

The payment experience for users can differ between countries. While some countries allow one-click payments, others with stricter regulations may require additional steps or verifications. Thus, during checkout, users may be prompted to:

- Share a PIN
- Share a Code from a Mobile Originated Message Consent
- Complete a payment while creating an Account

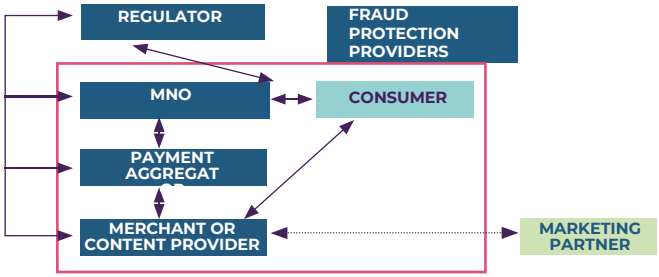
DCB Key Players

Although the transaction process appears seamless and simple for consumers, numerous essential players are involved in the Direct Carrier Billing process.

Key Players in Direct Carrier Billing (DCB) comprise:

- Consumers/Users
- Merchants selling Goods and Services
- Payment Aggregators
- Mobile Network Operators (MNOs)
- Fraud Protection Providers
- Regulators

Table 1. Mobile Content and DCB Payments Ecosystem:



Each player has varying levels of risk exposure, underscoring the importance of comprehending how fraud is handled in the mobile sector.

2.2. Fraud in the Mobile Industry

Fraud can harm businesses in various ways, emphasizing the need for companies to implement strategies to safeguard their customers, brand image, and marketing funds. It can affect consumers by leading to unauthorized transactions or the theft of sensitive data. Additionally, fraudulent activities can disrupt marketing campaigns and siphon revenue from merchants' advertising budgets.

Consumer Fraud

Even though DCB provides an extra layer
of security for consumers' financial data, there is still a risk of exposure to fraud. Some examples of fraudulent activities that can trick consumers into making unintended purchases include APK fraud, spoofing and clickjacking among others that will be later analyzed in detail.

Anti-fraud solutions are available to address these risks. Advanced tools assist merchants in identifying bots engaged in fraudulent activities and blocking such actions.

attempts, and reverse engineer existing threats.

It's also crucial for carriers to help consumers be informed shoppers. Consumers should check each statement to confirm that the charges are accurate and legitimate. To help consumers stay on top
of their transactions, carriers should provide clear and transparent descriptions along
with each charge.

If a consumer overlooks a purchase listed on a statement, it is essential for the provider to offer assistance in providing information and verifying its legitimacy. Unidentified charges might result from a forgotten transaction or indicate potential fraudulent behavior. To aid customers, sellers can:

- Customer care teams are available to assist with inquiries.
- Access MSISDN lookup tools.
- Employ third-party checkers, a common practice in countries with active regulatory associations.
- Ensure easy accessibility to proof of consent and visual reminders.

Marketing Fraud

Mobile ad fraud can significantly affect a merchant's marketing budget when fraudsters employ techniques like click spam, click injection, and SDK spoofing to boost impressions, clicks, and installations. In these scenarios, fraudsters can profit from advertising revenue for actions that were not genuine. While this initially impacts the advertising budget, in the long run, it can severely affect the data used for long-term advertising expenditure and targeting strategies. Therefore, it is crucial for merchants to actively supervise ad performance and seek assistance from professionals to monitor and analyze anticipated consumer behaviors.

How to Avoid Fraud

Fraud can have negative effects on both consumers and merchants, causing harm to the entire mobile content ecosystem. Therefore, it is advisable to bolster anti-fraud measures with human resources. Bringing in professionals who specialize in detecting fraudulent activities can prevent significant losses in the future. Consider hiring an in-house anti-fraud manager.

To enhance your company's workflow and monitor suspicious activity, think about incorporating support from independent anti-fraud companies. By integrating advanced targeting with Targetoo anti-fraud solutions, you can introduce valuable third-party solutions to boost your company's effectiveness.

Once a company has assembled a competent team to oversee anti-fraud measures, they can enhance the process to deter, examine, and combat fraudulent actions. The anti-fraud team can establish stringent regulations, blacklist partners involved in fraudulent activities, supervise traffic origins, and assess risks related to GEOs, billing, and traffic.

Fraud Tactics Explained

Following is an overview of the main types of DCB fraud occurring in the mobile payments ecosystem. This overview explains the detrimental impact on stakeholders and the recommended solutions for each type of fraud.

Fake Clicks			
Tactic	**Motives**	**Target**	**Solution**
Ad stacking Fake clicks on hidden ads below the visible ad **Click bots** Automated fake clicks **Click farms** Manual fake clicks, often low-wage **Click-injection** Malicious app generates fake clicks **Click hijacking** Redirects legitimate clicks **Click spamming** Overwhelm servers with fake clicks	**Profit** Exploiting ads for financial gain **Misallocation of Media agencies** Fake clicks distort budget allocation **Competitive advantage** Undermining rivals through fraud	**Advertisers** Wasted ad spend, reduced ROI **ad spend and publishers** Damage reputation, financial losses **App developers** Inaccurate metrics, revenue impact **Consumers** Poor User Experience, potential data compromise	**Robust fraud detection systems** Leverage machine learning algorithms, real-time monitoring **User behavior analysis** Detect deviations from baseline patterns **Continuous monitoring and analysis** Regularly analyze data, detect anomalies **Collaboration and information sharing** Share insights, best practices **Two-factor authentication** Implement additional security measures **Compliance with industry standards** Adhere to industry standards, regulations **Vendor and partner assessments** Assess credibility, verify fraud prevention **Educating users** Raise awareness, promote reporting

Consumer Manipulation			
Tactics	**Motives**	**Target**	**Solution**
Content locking Disabe the exit and back buttons for the user to subscribe to a service **Misleading ads** Misrepresent advertised content **Misinformation and misleading call-to-action** False info, deceptive call-to-action **Non-compliant ads** Violate industry standards **False endorsements** Falsely claim endorsements **Misleading incentives** Deceptive tactics for incentives **Hidden subscriptions** Conceal subscription terms **Unwanted redirects** Redirect users without consent	**Revenue generation** Illicit revenue through subscriptions, ads **Manipulating ad performance** Attract clicks, manipulate metrics **Competitive advantage** Gain edge by diverting traffic	**Consumers** Deceived, face financial loss **Advertisers** Financial losses, brand damage **Legitimate publishers** Reputation damage, trust erosion **Mobile network operators (MNOs) and carriers** Financial losses, disputes **Industry reputation and trust** Erodes trust, hampers growth	**Robust anti-fraud solutions** Use machine learning, anomaly detection, real-time monitoring **User behavior analysis** Monitor patterns, detect anomalies **Transparent and clear terms and conditions** Communicate transparent information **Compliance and regulation** Adhere to industry regulations **Vendor and partner due diligence** Assess credibility, verify anti-fraud measures **Continuous monitoring and analysis** Regularly analyze data, detect patterns **Collaboration and information sharing** Share insights, develop proactive measures **User education and awareness** Educate about fraud risks, report practices **Proactive monitoring of ad content** Ensure compliance, prevent misleading ads **Responsive customer care** Handle complaints, resolve issues promptly

Consumer Manipulation

Tactics	Motives	Target	Solution
APK fraud Modify legit apps to steal information **Bypassing payment pages** Redirect to fake pages for theft **Clickjacking** Trick users into fraudulent actions **Code injection** Add malicious code to steal information **Malicious apps** Create fake apps to mimic real ones **Remotely controlled fraud** Use remote access tools for control **Replay attacks** Intercept and replay legitimate transactions **Spoofing** Create fake sites/ apps to steal information	**Financial gain** Illegally obtain funds, generate revenue **Manipulating performance metrics** Inflate stats for financial gains	**Consumers** Experience financial losses, unauthorized charges **Mobile network operators (MNOs) and carriers** Deal with refunds, customer complaints, reputation damage **Content Service Providers (CSPs)** Face revenue losses, damaged reputation **Legitimate service providers** Reputational damage, reduced trust **Industry reputation and trust** Undermines trust, impacts growth	**Robust anti-fraud solutions** Use machine learning, AI, data analytics for detection **Two-Factor Authentication (2FA)** Implement additional security layer **Continuous monitoring and analysis** Real-time monitoring, analyze data for anomalies **User education and awareness** Educate about fraud techniques, encourage awareness **Vendor and partner due diligence** Assess partners' security, hold them accountable **Transaction monitoring and risk scoring** Evaluate fraud likelihood for each transaction **Collaboration and information sharing** Share insights, best practices in industry forums **Compliance with regulations** Adhere to industry regulations and privacy standards **Fraud investigation and response** Establish a team, respond to reported incidents **Customer care** Check Consumer Manipulation chart for details

Fraud Management

- In fraud management, companies can adhere to certain best practices:
- Choose an anti-fraud partner that is open to customers.
- Monitor live programs and stay informed about published content.
- Track traffic by analyzing buying patterns and conducting secret shopper assessments.
- Study data trends related to CTIT, new device rate, device sensors, ad tracking, and conversion rates.
- Keep up-to-date contractual agreements with mobile network operators for anti-fraud tools.
- Conduct thorough checks on partners to spot any history of fraud issues.

2.3. Compliance with DCB and mVAS regulations

To maintain consumer trust and prevent negative outcomes, it is essential to balance combating fraud with ensuring compliance with DCB and mVAS regulations in all markets.

Incurring complaints, refunds, and regulatory fines can have significant consequences. Additionally, carriers might suspend services if they encounter high volumes of complaints regarding DCB transactions on their networks. Furthermore, complaints can draw unwanted regulatory scrutiny, resulting in stricter legislation that could adversely affect businesses.

Here are some best practices to consider:

- Compliance with Mobile Carrier Regulations:
- Mobile carriers in different markets may have rules and codes of conduct that must be followed.
- Certain carriers may limit online payments to Direct Carrier Billing instead of PSMS.
- Most carriers mandate Double Opt-in, with many requiring PIN verification:
- For necessary PINs, they should typically be random and unique to the user, expiring if entered incorrectly or left unused for approximately 15 minutes. It's generally not allowed to pre-populate the PIN for the user.

- Regulations might demand additional evidence of consumer consent for charging, such as using a verifiable third-party PIN provider. Consent is typically shown by recording the key terms shown to the consumer and their agreement to make a purchase.
- The use of a fraud-blocking provider is becoming a requirement in numerous markets.

2. Countries often have content - specific regulations to take into consideration such as:

- · Gambling services will require registration and additional controls or may be banned completely.
- · Competition services are often restricted.
- · Adult services (pornography) are banned in many markets, particularly the Middle East; this often includes restrictions on the placement of adverts for other genres of service within adult sites or utilizing any adult images within the ad banners.
- · In countries where adult services are permitted, the rating of content may be restricted, X-rated content may be banned, and only less explicit glamour-style content allowed.
- · Fortune telling and horoscope services are often restricted. Where permitted, they should avoid advice on topics of health and finance.
- Advertising should always be truthful and informative, avoiding false claims or withholding essential information. Here are some key points to consider:
- When utilizing Marketing Affiliates for traffic generation, it is crucial to monitor the claims made on your behalf. Utilizing ad-scanning technology for spot-checking promotions is advisable.
- Social media platforms have seen an increase in misleading claims from affiliates, leading to customer complaints. These claims often promise non-existent rewards like free phones or virtual credits before users even reach the sign-up page.
- It is generally discouraged to target promotions towards minors. While enforcement may vary, European Union countries are typically bound by strict regulations prohibiting advertising to children.

- Generic advertising banners are discouraged as markets increasingly demand banners to be service-specific and include brand and price details.
- The placement context of banners can also be problematic. For instance, placing "Download Now" style banners on a website alongside unrelated video or music content might lead to violations for deceptive advertising.

4. Landing pages need to achieve informed consent to charge:

- Provide clear and transparent information about the charges, including the amount, frequency, and duration of the service.
- Price should be prominent and proximate
- to the call to action; this is often a very subjective area of regulations with a large degree of interpretation depending on country and operator. It is recommended to present key terms in clear contrast, and font sizes proportionate to the size of the call
- to action and other prominent promotional screen elements.
- Button wording should use payment terms. • You should give customers the ability to cancel their subscription at any time, and the Opt-out instructions should be visible on payment screens and receipts.
- Ensure that customer service contact details are operational and readily available. While standards may vary by country, it is typically recommended to offer a standard-rate or toll-free number that is staffed during business hours. Alternatively, if voicemail is an option, responses should be provided promptly within 24-48 hours.

5. Protect customer data from unauthorized access or disclosure; within Europe, the General Data Protection Regulations (GDPR) will apply.

*It is important to note that these are just some of the key compliance requirements for DCB and mVAS overseas. If you are considering offering these services, it is important to consult with a legal advisor to ensure that you are in compliance with all applicable laws and regulations.

2.4. DCB Geo Analysis

To get a concrete understanding of the mobile ecosystem and DCB, it's necessary to look at specific regions and countries. In doing so, it's easier to understand the nuances and factors prevalent in each respective area.

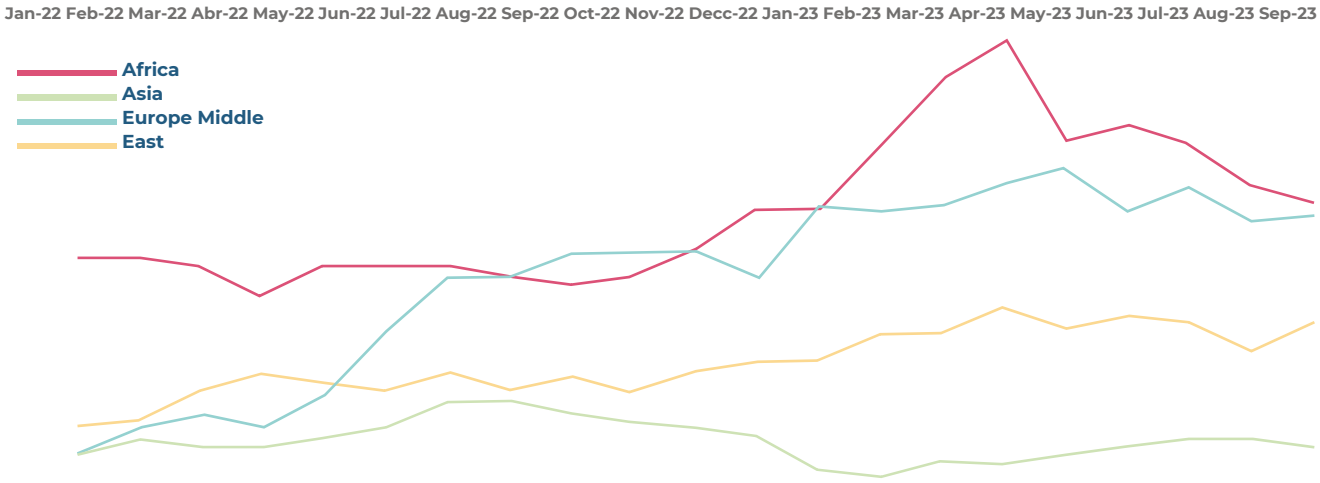
Targetoo has in-depth market knowledge of selected countries in Europe, MENA, Africa, and Asia.

In the specified regions, Targetoo managed over 200 active campaigns by October 2023, experiencing a 23% annual growth and expanding its reach to more than 430,000 average monthly subscriptions, surpassing last year's numbers by 20%.

DCB in Europe

The European DCB market is expected to grow to $17,649.7 million by 2027 at a 10.5% CAGR. Smartphones are the preferred choice for DCB payments, holding a 57% share, while tablets and other devices are projected to grow in usage.

Graph 2: Progression of Active Campaigns by Targetoo (January 2022 to September 2023)



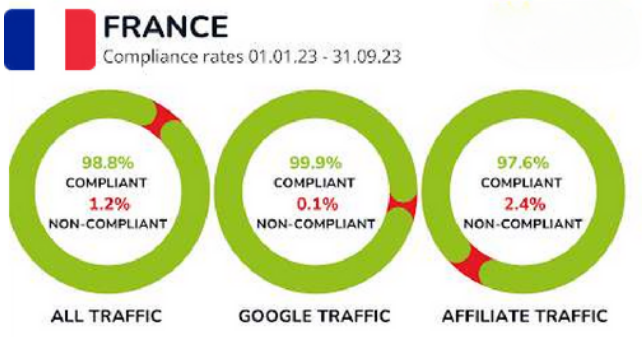
Total 119 138 147 139 163 185 219 213 217 210 226 234 245 278 309 340 305 302 304 267 271

In terms of content types, games dominate the market with a 52% share, followed by video in the second place with 27% of the share. Music, Lifestyle, and EPublishing follow the list with 10%, 5%, and 6%, respectively.

France

France stands out as the leading country for Targetoo, with 86 active campaigns in September 2023, marking a +19% increase compared to the previous year, and achieving an average of 21,888 monthly subscriptions. Despite some non-compliant activity displayed in the graph for France, the country maintains a high level of compliance. Targetoo highlights that the prevalent fraudulent practices involve sharing deceptive content to lure consumers.

Graph 3: Compliant vs non-compliant traffic



Regulatory Bodies and Compliance Requirements:
France maintains stringent regulations for mobile payments through various governing bodies:

Autorité de Régulation des Communications Électroniques et des Postes (ARCEP): ARCEP, an autonomous entity, regulates electronic communications and postal services in France. Its duties involve ensuring equitable competition, encouraging innovation, and protecting consumer rights. Registration with ARCEP is mandatory for Direct Carrier Billing or mVAS providers in the country.

Commission Nationale de l'Informatique et des Libertés (CNIL): CNIL is responsible for overseeing the management of personal data in France and establishing guidelines for its collection, use, and secure storage in compliance with the General Data Protection Regulations (GDPR) of the European Union.

Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF): As a French governmental body operating under the Ministry of Economy and Finance, DGCCRF

enforces consumer protection laws, promotes fair competition, and combats fraudulent practices.

France has established specific compliance requirements defined by key legislations.

For instance, the Code des postes et des communications électroniques (CPCE) regulates the telecommunications industry, specifying the essential requirements for Direct Carrier Billing and mVAS providers. Additionally, the **French Data Protection Act,** revised in 2018 to align with GDPR standards, emphasizes the protection of personal data.

In addition to legal frameworks, Direct Carrier Billing and mVAS providers must adhere to industry codes of conduct, which include:

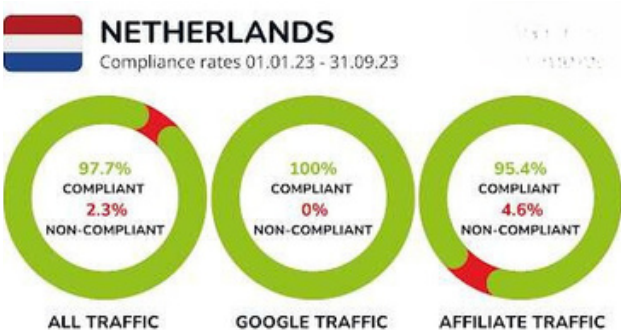
- **Fédération Française des Télécoms (FFT):** Acts as the representative organization for leading telecommunications companies in France.
- **Association Française du Multimédia Mobile (AFMM):** Supports the mVAS sector and brings together key players such as mobile network operators, content providers, service providers, and technology companies.
- **Association Française des Fournisseurs d'Accès Internet (AFA):** Uniting Internet Service Providers (ISPs) in France, which includes key players in the telecommunications industry.
- **Chambre de Commerce Internationale (CCI):** Supporting and advancing global trade and investments, providing a forum for business discussions, sharing best practices, and influencing policies.

Editors must transparently provide users with essential information, including details mandated by relevant laws such as LCEN Article 6 III and Consumer Code Article L.113-3. This encompasses service features, delivery conditions, and avenues for submitting claims (Chatel Law, Article 29, LME Article 87). For data-related matters or user communication services, editors must inform users of potential data usage (French Information and Liberties Act, Chapter 5). Additionally, if the service has specific restrictions, users must be duly alerted.

Netherlands

In September 2023, Targetoo in the Netherlands ran over 15 active campaigns and connected with an average of 2,858 monthly subscribers, demonstrating an 8% growth compared to the previous year. Compliance with regulations in the Netherlands stands at 97.7%, with recent changes from 2023 leading to minimal non-compliance rates across various traffic sources.

Graph 4: Compliant vs non-compliant traffic



Regulatory Bodies and Compliance Requirements

In the Netherlands, ensuring compliance with mobile payment regulations involving various regulatory authorities:

- **Authority for Consumers and Markets:**

This independent regulatory body oversees multiple sectors, including telecommunications and competition.

· **Dutch Data Protection Authority (Autoriteit Persoonsgegevens):** This authority enforces the General Data Protection Regulation (GDPR) within the Netherlands and sets the guidelines for the collection, utilization, and secure storage of personal data across the European Union. Compliance requirements in the Netherlands are anchored in the following legal frameworks. The **Telecommunications Act (Telecommunicatiewet)** governs the telecommunications sector, establishing prerequisites for Direct Carrier Billing and mVAS providers. Additionally, the Consumer Protection Act (Consumentenwet) regulates consumer protection in the Netherlands, delineating how companies must interact with their customers.

Direct Carrier Billing and mVAS providers must also adhere to industry codes of conduct established by:

- **The Dutch Consumer Association (Consumentenbond):** A non-profit organization dedicated to championing consumer rights and interests, which has been actively operating in the country since 1953.
- **Stichting Gedragscodes Mobiele Diensten (SGMD) or the Dutch Foundation for Mobile Services Codes:** This organization in the Netherlands oversees the adherence of mobile service providers to industry codes of conduct, established through collaboration between the mobile industry, consumer organizations, and the Dutch government. SGMD is committed to ensuring responsible and transparent practices in mobile service provision, including:
- **Code Development:** Collaborating with relevant stakeholders to create industry codes of conduct for mobile service providers, outlining guidelines and best practices for foundation members to follow.

° **Compliance Monitoring:** Monitoring members' compliance with established codes of conduct, investigating complaints and allegations of non-compliance, and taking appropriate measures to address violations.

- Dispute Resolution: Offering a platform for consumers to submit complaints and seek resolution regarding mobile services. SGMD ensures that member companies promptly and fairly handle consumer complaints, thereby aiding in the resolution process.

DCB in MEA

The MEA region is expected to achieve an impressive $5.8 billion by 2027, according to Juniper Research.
Paying for digital content through carrier billing has become a prevalent payment method in the Middle East. Even in 2020, the average revenue per paying user (ARPPU) for carrier billing in the Middle East and Africa amounted to $14.9.
The preference for mobile payments in this region continues to rise, with 64% of consumers increasing the use of at least one digital payment option, including Direct Carrier Billing (DCB).

Iraq

During September 2023, Targetoo owned 26 active campaigns in Iraq, with a 44% growth vs the previous year, reaching an increasing number of 39,138 average monthly subscriptions (+92% vs LY).

Iraq shows high levels of compliance for Google traffic, less so for affiliate traffic. Targetoo team has found that misleading advertising, coupled with services not permitted, drives the majority of fraudulent activity in Iraq. Mixed Content Portal presents the highest level of compliance issues, followed by games. Consumers are also at increased risk when using video, e-learning, media content portals and lifestyle.

Regulatory Bodies and Compliance Requirements

The **Communications and Media Commission (CMC)** in Iraq holds authority over the telecommunications and media sectors. Established under Law No. 89 of 2004, the CMC operates independently to regulate and supervise these vital industries. Their role encompasses ensuring equitable competition, safeguarding consumer rights, overseeing the radio spectrum, and fostering the growth of the telecommunications industry in Iraq.

For Direct Carrier Billing and mVAS providers in Iraq, compliance is essential with stipulations which are outlined in various legal frameworks, including **the Telecommunications Law No. 13 of 2001, the Consumer Protection Law No. 1 of 2006, and the Personal Data Protection Law No. 8 of 2018.**

Noteworthy points concerning Mobile Payment Services include:

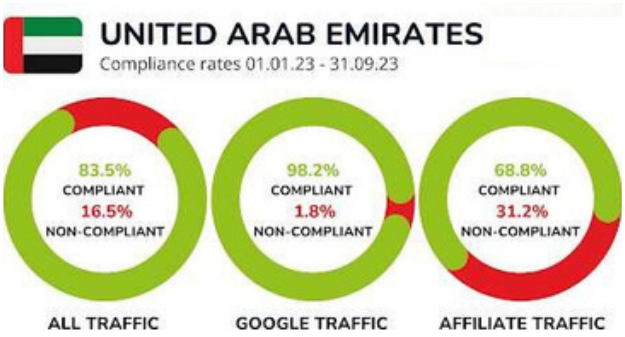
- Prohibition of adult content.
- Requirement for Arabic language usage.
- Subscription services are permissible, with a recommended 1-day free trial.
- Adherence to Islamic principles regarding content restrictions.

United Arab Emirates

As for the United Arab Emirates, by September 2023 Targetoo had 14 active campaigns, more than double the number from the previous year. Average monthly subscriptions increased to 4,621 showing a 420% growth.

The market compliance for UAE shows a compliant traffic of 83.5% with the majority of high-severity issues associated with non-Google traffic. While games are the category plagued by most problems, challenges also arise with other categories like media content portals, mixed content portals and quiz/competition among others.

Graph 6: Compliant vs non-compliant traffic



Regulatory Bodies and Compliance Requirements

In the UAE, the responsibility for ensuring compliance with mobile payment regulations lies with the **Telecommunications Regulatory Authority (TRA)** as mandated by Law No. 1 of 2006. This law serves as the governing framework for the telecommunications sector, setting the standards and guidelines that Direct Carrier Billing mVAS providers must strictly follow to comply with telecommunications regulations. Additionally, DCB and mVAS providers in the UAE are subject to the following regulatory provisions:

· **Consumer Protection Law No. 24 of 2006:** This legislation is designed to safeguard
the rights and interests of consumers in the UAE. DCB and mVAS providers are obligated to adhere to these regulations, which encompass principles of fair business conduct, transparent pricing, accurate product information, and well-defined terms and conditions for their services.

· **Personal Data Protection Law No. 5 of 2021:** This relatively recent law focuses on the protection of personal data within the UAE. Compliance involves implementing robust data protection measures, obtaining proper consent for data processing, and managing personal data in accordance with the law's stipulations.

Further considerations encompass:

· **Licensing:** Before commencing operations in the UAE, all mVAS providers are required to obtain a license from the TRA. This process is thorough, involving steps such as technical evaluation and financial auditing.

· **Registration:** Prior to offering services to the public, all mVAS providers must complete a straightforward registration process with the TRA, providing basic business information such as name, address, and contact details.

· **Tariffs:** All mVAS providers are mandated to invoice their customers according to tariffs approved by the TRA, ensuring accessibility and affordability of mVAS services for all UAE residents.

· **Quality of Service (QoS):** The TRA sets standards for the quality of service that mVAS providers must deliver to their customers. These standards cover various aspects, including network availability, response times, and data security.

• **Security:** The TRA requires mVAS providers to implement appropriate measures to protect customer data and privacy. These measures include data encryption, the use of strong passwords, and the implementation of intrusion detection systems.

· **Complaints:** The TRA provides a mechanism for customers to submit complaints against mVAS providers. All complaints undergo thorough investigation, and the TRA may take appropriate actions, such as issuing warnings or imposing fines.

DCB in Africa

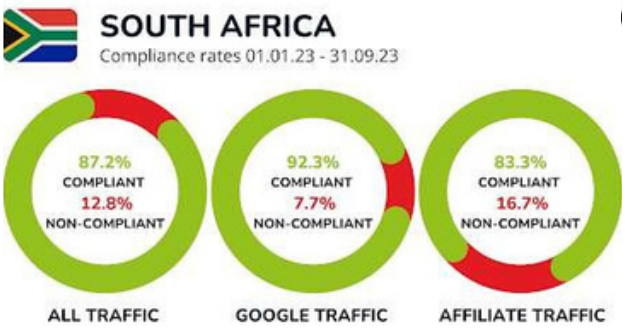
Since nearly 50% of the African population doesn't have a bank account, DCB is a promising avenue to increase purchasing power in the digital sphere. So, it's no wonder there's an expected 60% increase in mobile payments by 2025 in the African market.

South Africa

South Africa is the second strongest country for Targetoo, after France. During September 2023, the company had 75 active campaigns (+74% vs LY), while unlocking the power of more than 121,000 average monthly subscriptions with an increasing +34% growth compared to the previous year.

12.8% of the South African market has issues with non-compliant ad flows and landing/payment pages. According to our reporting findings, promotion pricing and misleading content are the major issues facing this area. Mobile personalization, video and games are the main categories struck predominantly with promotion pricing challenges.

Graph 7: Compliant vs non-compliant traffic



Regulatory Bodies and Compliance Requirements

In South Africa, ensuring compliance with mobile payment regulations involves the oversight of several authoritative bodies:

· **The South African Communications Regulatory Authority (ICASA):** Operating as an independent regulatory entity, ICASA is responsible for overseeing and regulating the telecommunications, broadcasting, and postal services sectors within the nation. ICASA mandates that mVAS providers secure either a license or registration, contingent on the nature of their services. The specific prerequisites and registration procedures may vary based on the type of mVAS and associated risks. Strict compliance with ICASA's regulations is essential to ensure legal operations and avoid potential penalties.

· **The Consumer Goods and Services Ombud (CGSO):** Operating independently, CGSO specializes in resolving consumer complaints related to goods and services purchases. Established under the Consumer Protection Act of 2008, CGSO serves as a vital guardian of consumer rights.

· **The Information Regulator (IR):** Functioning as an independent regulatory body, the IR is entrusted with safeguarding personal information and promoting access to information. Its establishment under the Protection of Personal Information Act (POPIA) of 2013 is instrumental in preserving data privacy.

· **Wireless Application Service Providers' Association (WASPA):** Additionally, mVAS providers in South Africa must attain

membership in WASPA if they offer services falling within WASPA's code of conduct. By becoming part of WASPA, mVAS providers pledge to uphold the association's code of conduct, which offers comprehensive guidance and best practices in areas such as service provision, billing procedures, customer care, and the resolution of complaints. Embracing WASPA membership and adhering to its code of conduct underscores mVAS providers' commitment to delivering responsible and ethical services within the mobile industry.

The essential compliance requirements for Direct Carrier Billing and mVAS in South Africa are meticulously outlined by the following laws and regulations.

The Electronic Communications and Transactions Act (ECTA): This legislative framework governs the telecommunications sector, outlining specific requisites for Direct Carrier Billing and mVAS providers.

The Consumer Protection Act (CPA): Serving as the guardian of consumer protection in South Africa, the CPA mandates the conduct of companies when interacting with customers.

· **The Protection of Personal Information Act (POPIA):** As South Africa's data protection law, POPIA sets forth unequivocal guidelines regarding the collection, utilization, and secure storage of personal data.

The Ivory Coast

As for Targetoo, during September 2023 the company had 3 active campaigns running and achieved 28,732 average monthly subscriptions, growing +96% vs the previous year.

Graph 8: Compliant vs non-compliant traffic

The Ivory Coast has issues with fraudulent activity, 15.7% of all traffic is non-compliant. Targetoo analysis reveals that most challenges arise from misleading content, but many cases also face issues with promotion branding and targeting children. The misleading

content is focused almost solely on quiz content, whereas promotion branding arises mainly from mixed portal content, sports and games.

Regulatory Bodies and Compliance Requirements

In Côte d'Ivoire, compliance with mobile payments is overseen by the following authorities:

· **Autorité de Régulation des Télécommunications et des Postes (ARTCI):** This principal regulatory body is tasked with supervising the telecommunications sector. Its core mission is to ensure the efficient operation, growth, and regulation of the telecommunications and ICT sectors in Côte d'Ivoire.

· **Commission Nationale de l'Informatique et des Libertés de Côte d'Ivoire" (CNIL-CI):** Serving as the national data protection authority, CNIL-CI is responsible for enforcing data protection laws in Côte d'Ivoire. The primary data protection law in the country is Law No. 2013-450 on the Protection of Personal Data, which establishes the legal framework for data protection and delineates the rights and responsibilities of data controllers and .subjects

Conseil National de la Consommation · A governmental entity dedicated **:(CNC)** to advance and safeguarding consumer rights and interests in the nation. It ensures equitable business practices, increases consumer awareness, and facilitates the resolution of consumer disputes.

The essential compliance requirements for Direct Carrier Billing and mVAS in Côte d'Ivoire are delineated in the following legal frameworks:

· **The Telecommunications Act (Loi n° 2014-581 du 24 décembre 2014 relative aux communications électroniques et à la poste):** This Act governs the telecommunications sector in Côte d'Ivoire, setting forth the prerequisites for Direct Carrier Billing and mVAS providers.

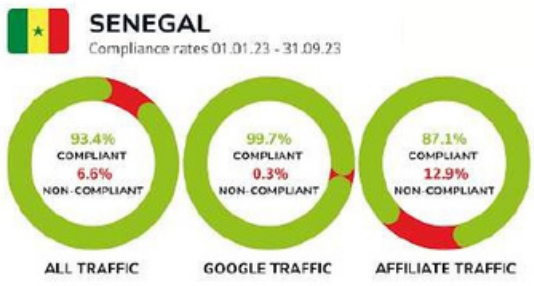
· **The Consumer Protection Code (Code de la consommation):** The Consumer Protection Code regulates consumer protection in Côte d'Ivoire, establishing the criteria for how companies must interact with their customers.

In addition to statutory laws and regulations, compliance for Direct Carrier Billing and mVAS providers also requires adherence to industry codes of conduct. These codes are established within contractual agreements by the Mobile Networks and Aggregators.

Senegal

In September 2023 Targetoo had 26 active campaigns running in Senegal, surpassing the previous year's amount by 48% and achieving 51,593 average monthly subscriptions (+47% vs last year).

Graph 9: Compliant vs non-compliant traffic



Currently, Senegal demonstrates good compliance, with Google traffic reaching 99.7% compliance and affiliate traffic at 87.1%. Targetoo reports indicate instances of fraudulent activity targeting children and disseminating misleading content, with the latter gaining prominence in August 2023. Users should exercise additional caution when making purchases in the games category.

Regulatory Bodies and Compliance Requirements

In Senegal, the telecommunications sector's regulatory landscape involves several entities:

- Autorité de Régulation des Télécommunications et des Postes (ARTP): Established in Senegal by Law No. 2011-01 on February 24, 2011, ARTP operates as an independent administrative authority. Its main role is to supervise and regulate telecommunications and postal services to ensure fair competition, service quality, and consumer protection. ARTP's key responsibilities include:
  - Regulation and Licensing: ARTP develops regulations, defines licensing conditions, and establishes technical standards for telecommunications and postal operators in Senegal. It grants licenses and permits to operators while ensuring compliance with regulatory requirements.

- Consumer Protection: ARTP safeguards consumer rights by enforcing regulations related to service quality, transparent billing, complaint resolution, and fair business practices.
- Commission de Protection des Données Personnelles (CDP): Responsible for data protection in Senegal, CDP oversees the implementation and enforcement of data protection laws. The primary data protection law in Senegal is Law No. 2008-12 of January 25, 2008, known as the Data Protection Law. This legislation defines the rights and responsibilities of data controllers and subjects.
- Conseil National de la Consommation (CNC): A government institution dedicated to protecting consumer rights and promoting fair business practices. Its main goal is to safeguard and advocate for consumer interests across different economic sectors.

The essential compliance requirements for Direct Carrier Billing and mVAS providers in Senegal are outlined in the following legal documents. The Telecommunications Act (Loi n° 2003-002 du 13 janvier 2003 relative aux télécommunications et à la poste) governs the telecommunications industry in Senegal and sets out the conditions for Direct Carrier Billing and mVAS providers. Additionally, the Consumer Protection Code (Code de la consommation) supervises consumer rights, detailing the standards for businesses in their interactions with customers.

Apart from these legal frameworks, specific obligations and expectations will be stipulated by Mobile Networks and Aggregators as part of contractual agreements.

DCB in Asia

The Direct Carrier Billing market in Asia is projected to achieve a value of US$ 35,700.1 million by 2027, experiencing a CAGR of 13.1% from 2020 to 2027.

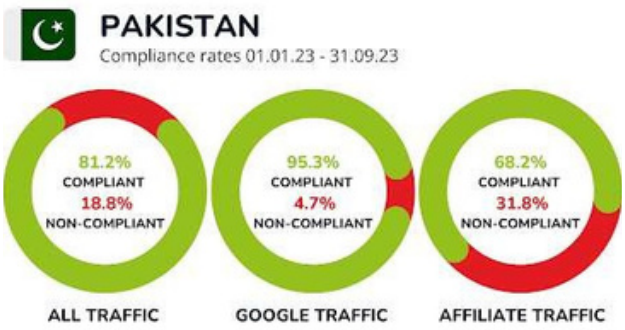
The Asia Pacific region is anticipated to be the fastest-growing market for Direct Carrier Billing, fueled by the rising prevalence of smartphones in developing economies and the growing collaborations between mobile network operators and digital content providers.

Pakistan

In September 2023, while the number of active campaigns by Targetoo decreased in the region, the average monthly subscriptions reached a significant 68,259.

Pakistan experiences significant issues with non-compliant affiliate traffic, 31.8%, bringing the over rate of compliant traffic to just 81.2%. As per the Targetoo report, the issues impacting Pakistan include promotion content, misleading content, and instances of targeting children. These issues become acutely more visible in the games and video categories.

Graph 10: Compliant vs non-compliant traffic



Regulatory Bodies and Compliance Requirements

In Pakistan, the Pakistan Telecommunication Authority (PTA) is responsible for regulating the telecommunications sector, which includes overseeing billing methods and payment systems. mVAS providers must register with the PTA to ensure compliance with applicable regulations, maintenance of set standards, and adherence to consumer protection requirements.

Providers in Pakistan must strictly follow these key regulations:

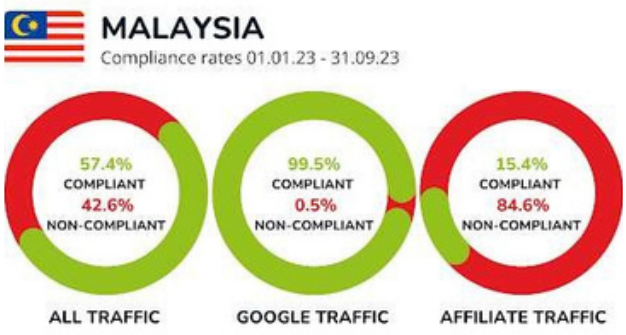
- Telecommunications Act 2005
- Consumer Protection Act 1985
- Protection of Electronic Transactions Ordinance 2002
- Personal Data Protection Act 2016

Although Pakistan lacks specific Mobile Payments Codes of Practice, adherence to industry standards is enforced through individual agreements with Mobile Networks and Aggregators.

Malaysia

Non-compliant activity is a significant problem in Malaysia, almost entirely generated by affiliate traffic with 84.6% of affiliate ad flows or landing/payment pages having compliance issues. These compliance issues infiltrate almost every category for DCB transactions. Per the information provided by Targetoo, topping the charts for fraudulent activity are transactions related to mixed content portals.

Graph 11: Compliant vs non-compliant traffic



Regulatory Bodies and Compliance Requirements

In Malaysia, the Malaysian Communications and Multimedia Commission (MCMC) is responsible for overseeing direct billing practices. The MCMC regulates the telecommunications and multimedia industries in Malaysia, ensuring compliance with regulatory standards and protecting consumer rights. These regulations aim to maintain transparency in billing processes and efficiently handle any issues or disputes related to direct billing services. Providers of Direct Carrier Billing (DCB) in Malaysia must adhere to the following legal frameworks:

- Communications and Multimedia Act 1998
- Consumer Protection Act 1999
- Personal Data Protection Act 2010

Those aiming to operate as mVAS providers in Malaysia must adhere to the licensing and registration requirements set by MCMC. The specific prerequisites may differ based on the services offered and the type of license required.

3. Conclusion

In 2015, mobile emerged as the primary online advertising platform. Consequently, the industry is now directing its attention towards combating fraud in the digital realm where the majority of transactions take place. Having the right partner can combat the adverse impacts of fraud, which is crucial as Direct Carrier Billing (DCB) gains prominence as a key payment method in various countries, each with distinct regulations and environments.

Targetoo has collaborated to establish itself as the top provider in the industry, supporting mobile companies in managing the entire customer journey from advertising to customer service. Their primary emphasis is on combating fraudulent practices.

Develops advertising solutions to increase acquisition.

- Executes successful retargeting campaigns to boost revenues.
- Enhances awareness and demonstrates performance through advanced monitoring.
- Offers brand protection for Mobile Subscription Services and DCB.
- Combats fraudulent activities using anti-fraud measures.
- Addresses issues stemming from fraudulent activities.
- Positions companies to excel as industry frontrunners.

In line with the aforementioned points, selecting a partnership with industry experts is crucial. They can assist you in meeting your requirements, safeguarding your interests, and improving your overall performance.

Targetoo is integrated with leading brand safety tools like Integral Ad Science (IAS) and others. Whether using pre-bid protocols or more simplistic brand safety solutions, we know what we are doing and we know how to keep your brand safe.

TARGETOO

Whitepaper Transparency and Brand Safe Advertising

www.targetoo.com