# Tabel of Contents

1. **INTRODUCTION** ..........................................................................................................................03
2. **UNDERSTANDING THE ECOSYSTEM** ..........................................................................................05
   2.1 Mobile Content Landscape ..........................................................................................................06
   2.2 Impact of fraud ...............................................................................................................................07
   2.3 Payment flows ................................................................................................................................08
3. **FRAUD TYPES** ...........................................................................................................................13
   3.1 Advertising fraud ...........................................................................................................................14
   3.2 Direct Carrier Billing fraud .............................................................................................................15
   3.2.1 Social ............................................................................................................................................15
   3.2.2 Technical ....................................................................................................................................16
   3.3 Who are the fraudsters? ..................................................................................................................17
4. **FRAUD MANAGEMENT** ..............................................................................................................18
   4.1 Technical Solutions – Best Practices .......................................................................................19
   4.2 Technical Solutions – Business Model ....................................................................................20
   4.3 Commercial Framework ...............................................................................................................21
   4.4 Self-Regulation .............................................................................................................................21
   4.5 Fraud Mitigation .............................................................................................................................22
   4.6 Checklist .......................................................................................................................................22
5. **USE CASES** ................................................................................................................................23
   Bouygues Telecom/Evina ......................................................................................................................24
   Indosat ..................................................................................................................................................25
   Mobilcom Debitel/Vene Overwatch .....................................................................................................26
   MTN South Africa/Secure-D ...............................................................................................................27
   Ooredoo Oman ....................................................................................................................................28
   Vodafone Idea/MCP Shield ..................................................................................................................29

**ANNEXES** .......................................................................................................................................30
   Technical Fraud Guide .........................................................................................................................30
   Glossary ...............................................................................................................................................35

**ACKNOWLEDGMENTS** ....................................................................................................................38
The mobile content market is 20 years old. Over its lifecycle, it has evolved considerably. It continues to serve an active customer base and is full of innovation.

However, where there are digital transactions, there is the risk of fraud. Mobile content is no exception. Unscrupulous individuals and criminal networks use ever-evolving methods to defraud customers, mobile content providers, payment aggregators and MNOs.

It’s a complex ecosystem with fraud happening at multiple layers. Some attackers target the advertising space – using technical methods to win pay-outs for bogus clicks. Others target the payment channel itself. Since many mobile content providers choose direct carrier billing (DCB) as their method of choice, this hits mobile networks and their partners especially hard.

DCB is fast and convenient for both merchants and consumers. Fraudsters exploit these qualities in two main ways.

The first is through social engineering, which they use to trick customers into unwanted purchases. The second is a more technical form of manipulation. Here, fraudsters use technological methods – bots, click farms etc – to receive illegitimate pay-outs. Obviously, the victims targeted differ according to the nature of the fraud. With social engineering, it’s end users. With technical manipulation, it’s MNOs.

However, the truth is that everyone loses. The erosion of trust affects all stakeholders:

- End users lose money
- MNOs lose revenue and incur extra customer service complaints
- Merchants lose brand reputation
- Aggregators risk market erosion

Anti-fraud companies are working hard to limit the impact of criminal attacks. But in this ongoing fight, it is essential that the entire ecosystem works together to combat fraud.
All stakeholders must be aware of the fraud types, and their differing impacts. Aligning on best practice limits the risk and helps everyone to stay ahead of the fraudsters. At the same time, any industry response should be measured. Regulators and MNOs need to be proactive while protecting the consumer experience and it’s important to take action against fraud that does not hinder honest stakeholders.

This whitepaper was developed by the Mobile Ecosystem Forum’s (MEF) DCB Fraud Working Group which brings together representatives from every part of the value chain. The aim is to share knowledge and best practice so that there is greater awareness and DCB fraud can be minimised.

Over the coming pages we will cover the following areas:

- **The ecosystem**
  This section introduces the key stakeholders in the mobile content value chain, describes typical payment flows and the impact of fraud on the ecosystem.

- **Fraud types**
  Here, we explore how the fraudsters operate – outlining the technical and socially engineered frauds that target mobile content advertising and the DCB payment channel.

- **Fraud management**
  In this chapter, we highlight best practice recommendations across technical, commercial and regulatory solutions to combat fraud.

- **Use cases**
  A series of MNO case studies demonstrating the impact of implementing anti-fraud measures.

- **Annexes.** Technical fraud guide and glossary.
UNDERSTANDING THE ECOSYSTEM
2. UNDERSTANDING THE ECOSYSTEM

2.1 Mobile content landscape

Fraudsters target all links in the mobile content value chain. Every stakeholder is affected.

This is especially the case when content providers use direct carrier billing. DCB is a relatively complex payment landscape with more players than there are in credit card, for example. These players have different exposure to risk, and contrasting incentives.

The value chain consists of:

- Consumer
- Merchant/content provider
- Payment aggregator
- MNO
- Fraud protection provider
- Regulator

Mobile Content and DCB Payments Ecosystem
2.2 Impact of fraud

Mobile content market fraud varies in its impact. When consumers lose out, the negative PR can be ruinous. Other more ‘invisible’ attacks on content providers and MNOs receive less publicity. But all fraud is serious. Here’s how the various stakeholders are affected.

Consumers
They lose money when they are tricked into unwanted purchases. They also lose trust in the DCB payment channel – and even in their own MNO.

Merchants
Merchants suffer in a variety of ways because they are responsible for the traffic they generate. They potentially lose revenue when defrauded consumers churn. They face fines, suspensions or service cuts by the affected MNO and by regulators. They suffer from damage to their brand reputation. They also face indirect longer-term impacts. More fraud can prompt regulators to add new steps to the payment flow (to keep it secure). But this added friction can cause consumers to abandon purchases.

Merchants can also lose out if their payment partner works with another merchant customer whose traffic has been overtaken by fraud. Measures taken against the under-attack merchant will affect its unaffected counterparts. They might find traffic sources blocked. They might turn to trusted networks (Google, Facebook etc) that offer less ROI.

Payment aggregators
A DCB payment aggregator provides a payment platform, which facilitates payments between MNOs and messaging providers. These companies can be vulnerable because they have no control over incoming traffic, yet pay a high price when traffic is fraudulent.

They might see their entire customer base eliminated when only a handful are directly impacted by fraud. This can erode the trust of the MNOs they work with, which is very bad news for aggregators. They depend on network connections – so nothing is more important than a healthy relationship with carriers. When trust goes, so does business.

DCB fraud detection providers
Fraud detection providers offer technical tools that detect and block fraudulent traffic. They occupy a central position in the DCB value chain. There are basic rules to selecting the right partner: a clear absence of conflict of interest; strong technical expertise, KPIs based on the image and the health of the market (see Chapter 3 – solutions).

MNOs
The MNO suffers the full brunt of bad user experiences. When there is fraud, the number of customer service calls increases. Unhappy subscribers churn to other networks. But there is also brand and reputational damage. It calls the survival of the DCB channel itself into question. Content is not an MNO’s core business and the risk is measured accordingly.
2.3 Payment flows

DCB offers consumers a quick and easy means of buying digital content, with the charge applied to their mobile phone account. To understand how DCB fraudsters work, it helps to understand the user experience and the payment flows on offer.

The payment flow which offers consumers the smoothest route between choosing to buy and agreeing to pay is the ‘one-click’ consent flow. Here, the user clicks on the ad and is directed to a payment page which explains the terms of service. He or she then clicks the subscribe button to confirm the payment. Sometimes MNOs may require the user to confirm the transaction twice (2-click flow).

The user’s payment experience varies depending on the country where the transaction takes place. In some countries the one-click flow is permitted only for specific categories of service.

In other markets regulators and MNOs have built in additional steps or specific requirements into this one-click flow to verify consumers. These extra steps result in three basic user flows. They are detailed over the next three pages.
## 1. Payment with PIN consent using MSISDN passthrough

The aim of MSISDN passthrough is to speed up and simplify a DCB payment, so the customer can pay without entering their mobile number. The MNO passes the MSISDN (mobile number) directly to the aggregator. (This method only works when the customer is on the mobile network, not on wifi.) In this flow, the user is required to consent by entering a PIN.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The merchant posts an ad</td>
</tr>
<tr>
<td>2.</td>
<td>The user clicks on the ad and is directed to a payment page (hosted by the MNO, aggregator or merchant), which explains the terms of the service</td>
</tr>
<tr>
<td>3.</td>
<td>He presses the subscribe button, which triggers the sending of a one-time PIN</td>
</tr>
<tr>
<td>4.</td>
<td>The PIN is delivered by SMS to the user’s phone</td>
</tr>
<tr>
<td>5.</td>
<td>He enters the PIN</td>
</tr>
<tr>
<td>6.</td>
<td>The user is sent to a new payment page, where the charge is confirmed</td>
</tr>
<tr>
<td>7.</td>
<td>The MNO, aggregator or merchant sends a ‘welcome’ message to the customer</td>
</tr>
<tr>
<td>8.</td>
<td>The merchant grants the customer access to its portal</td>
</tr>
<tr>
<td>9.</td>
<td>The MNO, aggregator or merchant sends the customer a payment receipt by text. This details the recurring charge.</td>
</tr>
</tbody>
</table>

---

### Payment with PIN Consent

[Diagram showing the process of payment with PIN consent]
2. Payment with Mobile Originated (MO) message consent using MSISDN passthrough

This method is very similar to the one above. This also uses MSISDN passthrough (to reduce friction). However, here the user gives consent by texting a confirmation message (rather than typing in a PIN). The customer responds to the initial service message by clicking 'yes'.

This migrates her to a payment page where she is invited to 'subscribe now'. However, there is no need for her to enter a PIN. Instead, her confirmation is enough to start the subscription. Some MNOs prefer this flow because they can store records of confirmation messages more easily than PINs. This makes for better auditing.

1. The merchant posts an ad
2. The user clicks on the ad and is directed to a payment page (hosted by the MNO, aggregator or merchant), which explains the terms of the service
3. She presses the subscribe button, which triggers the sending of a confirmation message
4. The message is delivered by SMS to the user’s phone
5. She replies ‘Yes’
6. The user is sent to a new payment page, where the charge is confirmed
7. The MNO, aggregator or merchant sends a ‘welcome’ message to the customer
8. The merchant grants the customer access to its portal
9. The MNO, aggregator or merchant sends the customer a payment receipt by text. This details the recurring charge

Payment with Mobile Originated Message Consent

FreeMsg: Please reply with YES to continue with your subscription to CONTENT for £/€ per week.

FreeMsg: Welcome to your CONTENT for £/€ per week from Branded Shop.
### 3. Payment with account creation consent

With this flow, the customer creates an account before making a payment. They choose a username and password, so there is no need for any further consent such as a PIN or 'yes' reply.

This reduces friction at the payment stage. That said, it is not a common method since few customers are prepared to create an account before discovering the details of the service.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>The merchant posts an ad</td>
</tr>
<tr>
<td>2.</td>
<td>The user clicks on the ad and is directed to an account creation page (hosted by the MNO, aggregator or merchant), which explains the terms of the service</td>
</tr>
<tr>
<td>3.</td>
<td>She fills in the details and clicks to submit</td>
</tr>
<tr>
<td>4.</td>
<td>She is sent to a new payment page, where the charge is confirmed</td>
</tr>
<tr>
<td>5.</td>
<td>The MNO, aggregator or merchant sends a 'welcome' message to the customer</td>
</tr>
<tr>
<td>6.</td>
<td>The merchant grants the customer access to its portal</td>
</tr>
<tr>
<td>7.</td>
<td>The MNO, aggregator or merchant sends the customer a payment receipt by text. This details the recurring charge</td>
</tr>
</tbody>
</table>

---

**Payment with Account Creation Consent**

![Payment with Account Creation Consent Diagram](image-url)
4. The DCB backend payment and receipt flow

<table>
<thead>
<tr>
<th>Payments</th>
<th>Delivery receipts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A consumer attempts to make a payment. The merchant instructs the aggregator to bill the consumer.</td>
<td>1. The MNO bills the consumer.</td>
</tr>
<tr>
<td>2. The aggregator sends a billing instruction to the MNO.</td>
<td>2. Providing there is no issue with the payment, the MNO confirms the delivery status as ‘success’.</td>
</tr>
<tr>
<td>3. The MNO bills the consumer.</td>
<td>3. The successful delivery status is shared with the aggregator.</td>
</tr>
<tr>
<td>4. The MNO charges the contract bill or debits the pre-pay account. This sends the customer to a new payment page, where the charge is confirmed.</td>
<td>4. The aggregator sends a payment receipt to the consumer.</td>
</tr>
<tr>
<td>5. The MNO sends a payment to the aggregator after 30 days.</td>
<td>5. The aggregator shares the successful delivery status with the merchant.</td>
</tr>
<tr>
<td>6. The aggregator makes an outpayment to the merchant.</td>
<td></td>
</tr>
</tbody>
</table>

---

**DCB Payment Flow**

- **Merchant**
- **Payment Aggregator**
- **MNO**
- **Consumer**
- **Online Advert**
- **Content Portal**

Payment Receipt

Outbound flow

Success & Return flow
FRAUD TYPES
3. FRAUD TYPES

There are two main types of fraud that impact mobile content stakeholders. One targets advertising and the other targets the DCB payment channel.

3.1 Advertising fraud

It is important to know who the parties are in mobile advertising and their basic commercial arrangement to understand why fraud occurs.

In the simplest form, there are publishers and advertisers. An advertiser is an entity selling a product that needs customers – for example, digital content merchants and app developers. A publisher is an entity that possesses these (potential) customers. Examples include website and app developers (with active user bases).

Advertisers will pay publishers for impressions, clicks, names, installs or subscriptions from potential customers.

In mobile content, fraudsters usually act as publishers in order to intercept these pay outs. They do this by:

- Generating pay-outs for bogus advertising clicks
- Generating pay-outs for bogus DCB transactions/subscriptions

Here are some common technical fraud types relating to mobile advertising:

**Click spamming/click flooding**

In the app install advertising space, ad networks have to decide which company is responsible for generating the download. They usually award the payment to the company whose ad generated the last click prior to an install. Fraudsters try to capture this last click by automating a large number of clicks on an ad without the end-user knowing.

**Click injection**

This is another type of ‘last click attribution’. Here the fraudster installs a malware app on a person’s phone. This knows when the user installs another app, and claims credit and payment for it.

**Device Farms**

A device farm comprises a large quantity of handsets that perform repeat actions – such as registrations, installs and engagement. This creates the illusion of legitimate activity. Advertisers pay out, but there are no real users.

* (See technical fraud guide annex for the full range of fraud types)
3.2 DCB Fraud

With ad fraud, attackers try to trick advertisers into paying for clicks with no users behind them. DCB payment fraud has a different target. Here, attackers trick customers or systems into making payments that are not intended.

They do this in two ways: via social engineering and by technical manipulation.

3.2.1 Social fraud

Here, fraudulent merchants use misleading information to deceive people. Obviously, this type of fraud cannot be tackled with technological methods. Instead, it falls to regulators (or stakeholders) to establish codes of practice.

There are four types of non-technical fraud:

Misinformation
Here, the merchant provides all the information that regulators insist upon. However, they make it incomplete or misleading. The aim is to dupe the customer into making a payment that they would not make if they were fully informed.

Examples of the methods used include:

- Very small or illegible pricing details
- Over emphasis on free trials
- Misleading calls to action eg “Play Now” or “Get It Here” that trigger a payment

Disinformation
Here, the correct payment information is not present. Fraudulent merchants omit pricing completely, make it incomprehensible or present purchase-critical information in other guises. Some unscrupulous merchants also hide billing receipts. Instead, they send them to destinations such as wifi routers. Similarly, they make it impossible for users who do discover a bogus subscription to unsubscribe.

Misleading incentive
In this fraud type, the customer responds to an advertised incentive, but the end result is not the one intended. For example, the user clicks on a message that says “You have won a prize!” or “A virus has been detected on your device”. After the action is taken, the fraudster forces the user to complete additional steps. This leads to an unintended purchase.

Trust manipulation
This is a kind of social engineering. Here, the fraudster uses various techniques to win the trust of the user. This can include assuming the identity of a contact or a trusted brand.
For example, the fraudster will set up a plausible-looking purchase page using a legitimate brand’s logo, font and colours.

The typical channels for this deception include WhatsApp chatbots and push-notifications. Sometimes these messages come from a contact whose account has been hacked.

At the end of the process, the user is tricked into making a purchase.

### 3.2.2 Technical fraud types

Technical fraud does not directly engage end users. Instead, attackers use technology to intercept a person’s phone and then start a subscription without the person’s knowledge.

There are many different ways to do this. But they can be broadly grouped into four:

1. **Malicious app fraud**
   - The fraudster creates a bogus app, which is programmed to set up a subscription/payment.

   The user downloads the app, believing it to be genuine. The app contains malware, and it processes a payment in the background.

   Malicious app fraud types include PIN and MSISDN entry fraud, remotely controlled fraud, click spamming, compromised handset and more.

2. **Code injection**
   - This is another way to inject malicious code in an end-user device. Here, hackers exploit a flaw in the browser or the server (via a header or URL). The user clicks on an interesting link that contains malware. The malicious code infects the user’s device and sets up a payment automatically.

   Code injection fraud types include tab nabbing, programmatic form submission and Javascript injection.

3. **Clickjacking**
   - This fraud intercepts the click. The user believes he has clicked on a specific button, but he has not. Instead, he has clicked somewhere else, which results in an unintended payment.

   The payment page is transparent. It sits behind a page that is more interesting for the user – a funny kitten video, for example. The user clicks to watch a video, and unintentionally makes a payment. Different clickjacking fraud types include i-framing, tapjacking and UI redress attack.
4. Spoofing  
Here, the hacker tries to steal/control the SIM/identity of the user in order to make a payment. For example, the customer uses a free VPN that shares her connection.

Fraudsters take control of this to set up subscriptions from other devices.

Different spoofing fraud types include MSISDN stuffing, header spoofing, UI redress attack, café issue, family fraud, wifi hacking, replay attacks, device farms.

(see glossary for the full range of fraud types)

3.3 Who are the fraudsters?

There is no typical DCB fraudster. Instead, they range from the tech-savvy individual to the sophisticated criminal syndicate.

At a MEF roundtable on the topic, experts discussed these disparate groups. It was suggested that most attackers were young people living in developing countries. They’re well trained and they earn modest sums.

Alongside these ‘side hustle’ fraudsters are more organised criminal groups. They target payment gateways 24/7 in an effort to find loopholes.

Both groups can easily share the malware they use to perpetrate technical fraud. The panel suggested there are at least 1000 different solutions and SDKs in circulation. And the price is coming down from thousands of dollars to $100.

Naturally, many of these SDKs are identified and put onto industry blacklists along with their creators. However, the fraudsters exploit flaws to counter this. They enter different names – or leave blank – the fields that might identify them as blacklisted developers.

Despite constant vigilance from Google, fraudsters do successfully upload malware apps to Google Play. They have even greater success on smaller independent app stores. And given the push by some major developers to switch to these portals (and away from Google Play/iTunes and their 30 per cent revenue shares), this malware threat might intensify.
FRAUD MANAGEMENT
4. FRAUD MANAGEMENT

In this chapter we explore the different ways the industry and its stakeholders must take into consideration when addressing mobile content fraud including technical, commercial and regulatory approaches.

4.1 Technical Solutions – Best Practices

Much has been done to strengthen the DCB ecosystem, including investing in anti-fraud solutions to support an ongoing detection programme. Here, we consider four simple best practices to deploy a successful anti-fraud solution.

<table>
<thead>
<tr>
<th>1. Know your providers</th>
<th></th>
</tr>
</thead>
</table>
| There are some basic considerations to make when selecting an anti-fraud partner. They should be independent. But if they do also provide content/traffic, there must be full disclosure to customers. | • Do a reputational analysis and scrutinise their historic record. Do regular updates  
• Use parameters such as public vs private, size, years in business etc  
• Ensure your partners adhere to rule sets  
• Confirm they know what's running on the network  
• Make sure your fraud detection provider has access to transaction and download data (ideally in real time)  
• Fraud detection should not be server to server (ie IP address, headers etc). Looking at IP addresses will catch just 10 per cent of fraud. Providers should inspect the device itself  
• Block bad actors. Make sure any party that has committed fraud cannot re-enter the product channel  
• Some fraudsters obscure their activity by reinventing themselves under a new guise. Make sure you link this activity to the original player. |

<table>
<thead>
<tr>
<th>2. Know your content</th>
<th></th>
</tr>
</thead>
</table>
| If vetting partners is important, so is vetting content. You should always know what is running on the product channel. | • Be aware of each purchase offer in the product channel prior to launch  
• Track all live programs  
• Remember the exceptions. Major storefronts such as Google Play and Apple App Store run independent onboarding processes. The verification authority cannot vet their listings |
3. Know your traffic

| Your market activity can tell you a lot about the presence or absence of fraud. You can assess this in three ways: | • Study transaction patterns and look for anomalies  
• Run secret shopper tests to see the customer experience up close – and make sure it is compliant  
• Do device-level monitoring and analysis |

4. Know your merchants

Make sure you can measure your merchants’ compliance efforts. Analyze their business results. Unusual spikes can reveal a lot.

4.2 Technical Solutions - Business models

What is the right business model for fraud detection providers? This is an important question. For obvious reasons, it comes down to incentives.

Consider the revenue sharing model. This risks incentivising the solutions provider to maximise the amount of fraud in the market. There’s a similar risk with conversion-based payment – where the provider is paid for each clean sale. Here, the better a company is at blocking fraudulent transactions, the less they get paid. Employees might be tempted to let through suspicious transactions to boost ‘clean’ sales numbers. There’s also a risk that the provider won’t block its own traffic but might hinder competitor traffic.

In both cases, more fraud = more money.

Another question concerns the ownership status of the fraud detection provider.

Some companies that sell anti-fraud solutions also sell traffic. In other words, the company that proposes to sniff out fraudulent is the same company that depends on that traffic to make money. The model for some of these companies is to provide anti-fraud solutions either at no charge or at a very low fee. They then monetise the traffic.

In a second scenario, they offer anti-fraud solutions that monitor only actors who are not their clients. In effect they are saying, if you become a client, we won’t track you. The conflict of interest is obvious. This is why the industry frequently refer to the above scenarios as ‘the fox guarding the hen-house’.

The key recommendation is to separate revenue from individual acts of fraud or from the total amount of fraud detected. Here the possible business models include:

• Monthly fee – A fixed amount that includes a defined amount of traffic or fraud checks.
• Click-based fee – a price for each fraud check (e.g. attempts on the payment page).
The same incentive issue applies to compliance service providers – or anybody in charge of verifying products. In short, their business model must not be tied to DCB revenue. They should be independent and transparent. And they should erect a firewall between their compliance activity and any conflicting business services.

4.3 Commercial Framework
A technically advanced anti-fraud solution can deliver best results when it is part of a commercial landscape optimised to accommodate such solutions – and aimed at preventing fraud. This requires the adoption of non-technical measures such as:

4.3.1 Contractual measures
The mobile payments ecosystem is governed by complex contracts, with annexures and schedules. These contracts have historically been focused on defining the commercial relationship and on service delivery specifications. They do not typically include rights and obligations related to the prevention of fraud. In mature DCB and/or PSMS markets, these contracts are often based on templates that predate the rise of mobile payments fraud as we know it today. Stakeholders should therefore review existing contracts and explore adding anti-fraud components such as:

(a) a clear definition or reference to mobile payment fraud
(b) an obligation on one or both parties to take reasonable steps to prevent fraud
(c) the right to investigate transactions suspected to be of a fraudulent nature
(d) sanctions or recourse in the event of transactions found to be fraudulent
(e) the obligation to implement a technical anti-fraud solution

4.3.2 Due diligence
A contract alone, however robust, is never a foolproof prevention tool. A pre-contractual "Know Your Customer" exercise could expose parties with previous convictions or a history of mala fide fraudulent activity in other markets. Parties who take the prevention and mitigation of fraud seriously are unlikely to consider such due diligence a barrier to entry.

4.4 Self-Regulation
It is essential that all stakeholders work within the relevant national regulatory environment. A key goal of this paper is to help inform regimes worldwide. Self-regulation and cross-stakeholder knowledge sharing also help. In markets where there is no external compliance body, forming a self-regulatory organisation can help bring together relevant stakeholders with the aim of defining the outlines in which consumers as well the industry can remain protected. The primary benefit of self-regulation is the ability to respond and adapt to market changes in a swift and agile manner.

One such example can be taken from South Africa’s Wireless Applications Service Providers’ Association (WASPA), the country’s non-profit regulator of DCB services and champion of consumer protection. WASPA’s members consisting of digital content merchants, payment aggregators and mobile network operators have successfully
responded to market threats on various occasions. In 2014 the industry body introduced a “three-strikes” warning system to deter and ultimately clamp down on the use of misleading affiliate marketing. More recently it amended its Code of Conduct to include an obligation on its members to “take reasonable steps to prevent their networks and systems from being used in a fraudulent manner”, a measure which was accompanied by the publication of Best Practices For Fraud Prevention.

Similarly, The Netherlands’ Stichting Gedragscodes Mobiele Diensten has in its Code of Conduct included a responsibility on service providers to “implement an anti-fraud monitoring system for Mobile Internet Services for detecting and stopping fraud.”

### 4.5 Fraud mitigation

Preventing fraud is the priority. But it’s also important to have a procedure for when it does occur. Here are some guidelines

- Keep an audit of all communications. This should cover notification to resolution.
- Demonstrate your strategy for mitigating fraud
- Have shutdown process in place
- Keep lines open with the verification authority so you can resolve the problem quickly
- Give the verification authority the ability to shut down the merchant service quickly
- Do follow-ups to make sure shutdown content has not returned

### 4.6 Anti-fraud checklist

<table>
<thead>
<tr>
<th>Don’t Panic! Fraud is part of all payment methods and can be handled.</th>
<th>Audit your risk Assess the threat by geography, traffic sources, service type or billing flow.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t believe fraud won’t happen to you Fraud impacts every link in the DCB value chain. No one is immune.</td>
<td>Be proactive Put measures in place to stop fraud before it occurs.</td>
</tr>
<tr>
<td>Don’t trust any traffic by default Do not assume your partners will clean your traffic before it arrives. Be vigilant.</td>
<td>Analyse traffic and conversion patterns Monitor your traffic and your ARPU to detect anomalies.</td>
</tr>
<tr>
<td>Take time to pay your traffic sources Analyse and validate traffic before you pay for it.</td>
<td>Set up a firm contractual framework Put in place strict sanctions against any partner that sends you fraudulent traffic.</td>
</tr>
<tr>
<td>Organise your team Put someone in charge of anti-fraud management and create a fraud management process.</td>
<td>Use independent cybersecurity experts Fighting fraud is highly technical. There are specialists that can help. Benefit from their experience and knowledge.</td>
</tr>
</tbody>
</table>
USE CASES
5. USE CASES – FIGHTING FRAUD

**Bouygues Telecom/Evina**

In 2018, a sudden rise in DCB-related customer complaints pushed Bouygues Telecom to reconsider its anti-fraud strategy. It put in place several measures. It asked DCB merchants to limit traffic acquisition to high controlled sources (e.g. Google, Facebook). It also reinforced responsible messaging on payment pages.

After nine months, the results were unsatisfying, so Bouygues introduced One-Time Passwords (OTP). Regrettably, this policy drove down purchase volumes yet had little impact on complaints.

In Q4 2018 Bouygues implemented the Evina anti-fraud system in Q4 2018 and the fraud rate fell from 14 per cent to one per cent. The complaint rate was halved. There was no adverse impact on legitimate purchases. In fact, transactions started to increase thanks to a cleaner payment flow (without the need for OTPs).

Franck Semanne, head of carrier billing at Bouygues Telecom, says: “Faced with a strong increase in complaints and without being able to explain the cause with certainty, we were considering stopping the invoice payment solution. The use of Evina allowed us to restore the click-flow. We were especially impressed by the purchase increase. This collaboration has saved the VAS market at Bouygues Telecom. Today I have a healthy relationship with my merchants, I am able to discuss fraud with them based on factual data, and we can work together in confidence to protect the end-user.”

<table>
<thead>
<tr>
<th>Complaint Rate Divided by 2</th>
<th>Purchases Multiplied by 5 compared to when OTP was active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud rate decreased From 14% to 1%</td>
<td></td>
</tr>
</tbody>
</table>
Indosat

In 2019, Indosat Ooredoo made a stand against rising levels of VAS fraud. The high rates – triggered by misleading product descriptions and acquisition bots – were causing the MNO problems on many fronts.

Users were sharing stories on social media, and churn rates were rising. In Indonesia, it is comparatively easy to switch carriers. Unhappy customers were responding to fraud by buying new SIMs from rival MNOs. Indosat Ooredoo decided to take control of the payment process for all content provider transactions. It advised content partners they could only advertise products with a visual component (to counter misleading descriptions). It then mandated that every banner-click would route through to its own app, where the consumer would complete an OTP payment process in a controlled environment. In addition, subscriptions could now only last for 90 days. After this point, the customer must actively renew.

The strategy worked. At the peak of the problem, Indosat Ooredoo was receiving 700 calls a day about questionable subscriptions. Nearly a year later, it takes about 60 such calls. However, this very important and necessary decision reduced Indosat Ooredoo’s VAS revenues to 33% but it helped in improving customer satisfaction and rebuilding trust.

The company focused on building new partnership models and services that drive consumption and purchases of data. It teamed up with Facebook and Snapchat to make it easier for customers to engage with social media (and thereby purchase more gigabytes). It worked with Google to support voice search for users that still use USSD services. And it also launched a free-to-play games portal to encourage the digital entertainment habit among subscribers.

Sudheer Chawla SVP of digital services at Indosat Ooredoo, says: “I still believe VAS has a future, and I want to help honest content partners. We are a Customer first Operator and there is no room for fraud. We are and will continue to apply the best possible methods to prevent fraud and deliver a clean user experience building new kinds of digital services that drive data growth, usage and engagement.”
Mobilcom Debitel/Vene Overwatch

Mobilcom Debitel is the largest MVNO in Germany, with 9.5 million mobile customers. It operates its own payment gateway, and also manages its own checkout platform for micropayment, ticketing, gaming and mobile content.

The MVNO was aware that the payment gateway was at risk from unscrupulous actors. It wanted to reimburse customers for existing fraud and prevent further harm. It also wanted to protect its reputation and reduce the cost incurred by customer complaints.

Mobilcom Debitel implemented Vene Overwatch into its payment gateway to minimize false positives and not impact legitimate purchases. After a two-week installation phase, blocking of fraudulent transactions started and traffic and revenue dipped slightly. But after week four, traffic returned. After 10 weeks the impact showed the following improvements:

- Share of ‘good’ traffic on the gateway: 80 per cent up
- Customer complaint numbers: down more than 40 per cent
- Customer complaint costs: down more than 20 per cent
- Revenue fell by nearly 30 per cent after week 4. By Week 10 it is almost back to normal.

![Traffic Quality, Customer Complaints and Costs, Revenues](chart)

- Tool is learning
- Not blocking
- Market Participants learned and send good-quality traffic at high volumes
- Traffic pays off for them, revenue goes up
- Traffic doesn’t convert into sales
- Antifraud Tool started blocking
MTN South Africa/Secure-D

MTN, one of the leading mobile operators in South Africa with 30 million cellular connections, turned to Secure-D in August 2018 to improve its fight against fraud.

MTN was receiving high levels of complaints about unwanted subscriptions because over 90 per cent of all mobile transactions attempts were fraudulent. Fraudsters had developed malware apps that were barely detectable to the user. Once activated, these apps began racking up bogus charges.

MTN decided to implement Upstream’s mobile anti-fraud platform, Secure-D which combines machine learning algorithms with payment processing workflows to identify and block fraud in real time. Its clearing process ensures no user is charged until the validity of the subscription has been certified.

At first MTN’s blocking rates were over 90 per cent. Mobile transactions are now processed via applied machine learning and behavioral analytics that highlight threats. After two months, business partners adjusted and improved their traffic mix.

After just five months, MTN achieved five times the number of activations versus the start of the project, and blocking rates dropped under 50%. As fraud rates dropped, so did the number of customer complaints. Calls about unwanted subscriptions fell by 75 per cent in the first six months of the project. MTN later extended Secure-D’s fraud protection to cover USSD.
Ooredoo Oman

Ooredoo Oman is currently experimenting with a number of anti-fraud solutions having switched to a one-time password only transactional flow in Q2 2020.

The MNO took the decision to add the OTP step to its payment process in response to rising complaints through 2019. At one point, complaints about unintended subscriptions comprised 12 per cent of all calls to customer care.

Following the mandate of OTP, Ooredoo Oman saw these numbers fall. By October 2020, just four per cent of complaints were about subscriptions – and most of these came from customers who needed help leaving a longstanding service rather than closing a new one.

So the strategy worked. Fraud dwindled. But so did revenue – Ooredoo Oman believes VAS income has fallen by up to 65 per cent.

To address this, the MNO tried many strategies to mitigate the fraud without damaging ‘honest’ traffic at the same time. It advised VAS companies to use Google Ads only, rather than affiliates. It built its own in-house blacklisting system (though it abandoned this when it found it was blocking legitimate traffic). It has also begun working with a ‘master aggregator’ to handle the digital acquisition on behalf of selected VAS partners.

Now, Ooredoo Oman is appraising one of the industry’s technical anti-fraud solutions – which is only became aware of thanks to the work of MEF’s anti-fraud working group.

Jalal Al-Amri, Senior Product Manager for VAS and DCB at Ooredoo Oman, says: “We want to help the VAS business to grow. To do that, we need to find systems that can provide a frictionless UX for our good partners while keeping a safer OTP flow for the rest. MEF has helped us understand the options, so that’s what we are working towards now.”
Vodafone Idea/MCP Shield

In India, Vodafone Idea received so many DCB complaints, it shut down almost all value-added services completely. To address the problem, it implemented MCP’s Insight Shield product on its main VAS platform.

Shield exposed a lot of fraudulent traffic – over 100,000 attacks per hour. It identified the source of the fraud as being mostly from affiliates, but occasionally from legitimate partners. The fraud attempts shared similar characteristics:

- Mostly from APKs
- Started at weekends
- Short-lived in nature – “get paid quick and get out”

Alarmingly, the fraudsters also attempted DDoS attacks in order to stop the anti-fraud platform blocking instructions to Vodafone in real-time/live.

Shield detected that these attacks came from 21,200 devices pinging through a single event, multiple times. At peak, there were 2600 events per second – all from one ‘family’ of APKs. The top handset used was an Mi-4c clone – most likely a compromised handset with a Chinese chipset that had been factory-hacked.

By implementing the anti-fraud solution, the attacks failed and Vodafone has since deployed the Shield platform to cover additional services. It is now on-boarding a new set of partners in order to address all 330 million subscribers.

Idea’s senior VAS director says: “We started our Proof of Concept with MCP Insight in late December and ran live traffic until now. We were happy with the solution and are aware of multiple attacks which the system has blocked and continues to block successfully on a constant basis. The Idea part of our group has also integrated the solution on its own gateway.”
Combatting Fraud in Mobile Content

ANNEXES

Technical Fraud Guide

1. Commonly Used Descriptions APP Malware

Coming mostly from older Android devices, there are three types of Malware in the market:
- Malware unknowingly installed by the users
- Existing Apps that are ‘co-opted’ (taken over by malicious players) and modified to commit fraud, so as soon user updates they get the malware on their device
- Existing or new apps that downloads dex (executable binaries).
- Apps that are downloaded from alternative app-stores or are sideloaded

In the last case, fraud can be committed (a subscription made) and the fraudulent Dex is deleted. In all cases there can be a delay (up to weeks) between install/update and first fraud attempt(s). In all cases related to Gateway endpoints, the malware instantiates an open (but usually unviewable – if someone is actually watching) web view using the native, or some other browser.

There are two types of fraud activity:
1. APK communicates with a ‘command and control’ server to receive the fraud ‘instructions’ – “go to this site, click this button etc.”
2. APK communicates with a control server and acts ‘dumb’ – allowing the control server to instantiate the instructions remotely while the device/APK acts dumb.

A single APK can attempt multiple subscriptions at any one time – this was quite prevalent in South Africa some time ago. It can also dial premiums service numbers and premium SMS.

APK Malware Blacklists - APK is uniquely identified mostly by its package name, it has been observed that fraudsters would create multiple copies of same APK with different package names and also package name can easily be spoofed and a spoofed package name could reflect a legit package name/APK as well. Therefore, appearing on a blacklist should not be the only ‘reason’ used to block.

Multiple APKs – Similar Pattern - Normally these types of Apps are controlled by single source via command and control structure.

Single APK – Different Device fingerprinting Data from Same Device - An APK trying to pretend as coming from different devices but actually it’s a single device.

Browser Exploits

Browser exploits used for questionable code execution on landing pages.

Click Farms

Click farms usually try and tap with lucrative payouts by changing their IP addresses using VPN or Proxy software, often hiding their activity, and resetting Device Parameters.

Click Injection

Click injection is a sophisticated form of click-spamming. By publishing a high-effort Android app that uses one of two distinct exploits to detect when other apps are downloaded on a device and trigger clicks after the user already made the decision to download and use an app.

Click Spamming

Click spamming (also known as click flooding) is a type of mobile fraud that sends a large number of fraudulent clicks on an ad without the user knowing, in hopes of capturing the last-click prior to an eventual “organic” install.
Compromised Handsets
In some markets handsets are pre-hacked and primed for fraud, once sold to consumers. “PHA family—Chamois—that we previously discussed publicly. Chamois apps are pre-installed on popular devices from different OEMs that didn’t carefully scan for malware. As a consequence, users are buying compromised systems. When users start up their new devices, the pre-installed Chamois apps (usually disguised as system apps) download and install PHAs and other apps in the background.” – Google Android Security 2018 Report Final

The following system apps are known to have been compromised:
- com.android.settings
- com.android.systemui
- com.android.browser

As mentioned above – blacklisting these apps will not be an effective solution – their attempts need to be programatically detected in real-time.

Device Farms
A device farm is a location wherein fraudsters repeat actions – such as registrations, installs and engagement – to create the illusion of legitimate activity, draining advertising budgets. Device farms maintained for the purposes of ad fraud are illegal in much of the world. As mobile advertising budgets have grown, device farms dedicated to mobile fraud have grown increasingly common.

Dispatch Proxy (>1 IPs per single TX)
Requests initiating from Gateway IP and getting processed from another remote server IP. This is to spoof gateway IP for Landing page and then serving the rest from command and control server.

FPS Attacks from Landing Page
In this scenario they put the system under pressure to get desired result, mostly, applications of asynchronous nature are exploited to trick the application into performing malicious events. The primary objective of the attack is to put the FPS under pressure and ideally, pull it down (i.e. – all the fraudulent traffic breaks through successfully).

FPS Replay Attacks
This is a combination of both replay and DDoS attack, where thousands of events with same parameters arrive on the gateway in a short period of time.

Header Spoofing
Spoofing of Headers underlies most fraud occurring, specifically on the Android platform. Theoretically all header parameters are hackable, header spoofing can be enabled by,
- Lack of Encryption in the Communication
- Improper SSL Error Handling
- Lack of Content Loading Validation

iFraming or Clickjacking
When an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page.

IP Spoofing
Spoofing IP Address to Bypass Weak Gateways.

IVT
Invalid Traffic (IVT) Invalid Traffic (also called Non-Human Traffic) is traffic implementing bot activity on pages.

JS Code Injection
Anonymous piece of code injected into page to perform inappropriate tasks.

MSISDN-Stuffing on Gateway
Payment fraud multiple scales depending
upon the relative weakness of the target gateway.

Highly vulnerable gateways are where the transaction presents with no more than two correct parameters: A Gateway IP address; and some unique identifier. The weakest gateways allow reuse of the identifier, Gateway IP address and allow MSISDN-stuffing (where the fraudster inserts a MSISDN – even randomly) into the headers. So, a common fraud is where a server or phone with a single SIM card (using its Gateway IP address) generates serial requests to subscribe a user. Gateway IP addresses / ranges are also traded on the black market as well as legit MSISDN.

Additionally, there are Gateways that will accept subscription attempts even when the IP address is off-Gateway or even outside of the country.

No User Events Anomalies
There are still large numbers of cases where malware, mostly, presents onto payment pages. Although declining in recent months (2020) these APKs are failing to generate any events that look remotely like User events or interactions and seem to attempt to complete the transaction by expediting a FORM POST method on the payment page.

PIN and MSISDN-entry fraud
Using Malware generally, fraudsters can steal user’s MSISDN and access SMS inbox, read a PIN and ‘enter’ the PIN into a PIN-entry form on the APK’s view. Therefore, any PIN or MSISDN Entry endpoints need to be protected. This is particularly the case when a fraud system detects fraud and the operator or aggregator redirects to a PIN-entry mechanism. Also, both APK and browsing can interact simultaneously.

Programmatic Form Submission
Subscription Form Submission without the user being aware.

Programmatic Form Manipulation & Submission
Subscription form submission after changing parameters but keeping necessary information required to authenticate the request this method is used to exploit weak gateways.

Remotely Controlled Fraud
Fraudsters utilise simulations – simulated devices running off a central server – to generate fraudulent impressions, clicks and even in-app engagement. Some fraudsters will even create deep device metadata profiles in an attempt to make simulated devices appear real.

Replay Attacks
A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

Mostly these are cases of headers spoofing, MSISDN-Stuffing on Gateway and generally exploiting gateway vulnerabilities etc.

Tab Nabbing
Exploit and phishing attack used to fool users or redirect users to some fraudulent site without the user knowing. A payment page opened in a new tab can be controlled by the parent window and the fraudulent site can expedite a subscription.

Timeseries Anomalies
Too many requests coming in a short period of time, mostly from same IP address, but sometimes from multiple IP addresses but with similar patterns. Also, there are some advance cases detected here, where it uses the combination of above techniques, both the IP address and the engagements are mixed.
Wifi Hacking / Café Issue / Family Fraud
First reported in UAE some time ago, in some GEOs where IP access is shared among multiple devices, thereby allowing Gateway access and MSISDN-identification to be mis-allocated to multiple handsets.

2. Anomaly Types
Background UI Rendering Detections
Where payment or landing pages are rendered but impossible to view by a human.

Bot Activity
Where non-human events are detected, it also includes form submission without user events detection.

Blocked Platforms and User-agent issues
Where non-mobile platforms and/or user-agents are being detected

Device Fingerprinting Anomalies
Problems with Device identification

Headless / Emulators
Spoofing or continuously updating parameters to avoid detection as "pretend" devices. Specific headless browsers are identifiable

JavaScript Engine issues
Where JS load/Rendering is deliberately interfered with.

Parameter Faking (Catchall) – Miscellaneous
Where parameters or headers are being changed or added

Real-time patterns Identification
Where events and data are grouped to indicate programmatic usage. This can include where fraudster is learning params the Fraud system is collecting and with what frequency.

TCP/IP Anomalies
Where a specific IP address is being used in such a way as to suggest abuse.
## 3. Fraud types by usage

<table>
<thead>
<tr>
<th>Fraud Type</th>
<th>Mixed Usage</th>
<th>JQuery Engine Issues</th>
<th>Bot Activity</th>
<th>Background UI Rendering Detections</th>
<th>Headless/Emulators</th>
<th>TCP/IP Anomalies</th>
<th>Blocked Platforms and User-Agent Issues</th>
<th>Device Fingerprinting Anomalies</th>
<th>Real-time Patterns Identification</th>
<th>Parameter Faking/Catchall</th>
<th>Adaptive Behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Malware</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Remotely Controlled Fraud</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Replay Attacks (single event repeats)</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Real-time Patterns Identification</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Post Event Patterns Identification</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>BOTs</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Time Series Fraud</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Despatch Proxy (&gt;1 IPs per single TX)</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Spoofing</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>MSISDN-stuffing</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>JS Code Injection</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Click Jacking</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Touch Jacking</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Tab Nabbing</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Bot Nets</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Emulators</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Browser Exploits</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>iFraming</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>IVT</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Click Spamming</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Click Injection</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Device Farms</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Click Farms</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Programmatic Form Submission</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Programmatic Form Manipulation &amp; Submission</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>
Glossary

**Affiliate Marketing**: an arrangement through which an online retailer or merchant pays commission to an external third-party partner for traffic or sales generated from its referrals.

**Affiliate Marketing Partner; Affiliate**: an external third-party partner which refers traffic or sales to an online retailer or merchant’s website or mobile payment page.

**Anti-Virus Software**: Software designed to protect internet-connected devices, including mobile devices, from malicious software, also known as malware, or viruses. See also SMS Malware.

**ARPU; Average revenue per user (ARPU)**: the total revenue divided by the number of subscribers.

**Billing Instruction; Billing Request**: a request submitted by a merchant to a payment aggregator to bill a consumer. The payment aggregator relays the request to an MNO which will then attempt to bill their customer, in line with the specific request initiated by the merchant.

**Billing receipt**: [See Delivery Receipt].

**Chatbot**: a computer program designed to simulate conversation with consumers, especially over the internet.

**Consumer**: an individual who purchases goods and services for personal use.

**Content Portal**: an online walled environment, which could be protected by a pay wall, for example.

**Content Provider**: [see also Merchant].

**DCB**: [See also Direct Carrier Billing] Charge to Bill, Charge to Mobile.

**Delivery Receipt (DLR); Billing Receipt**: A receipt to confirm that a message has been successfully sent by a messaging provider or that a message has been successfully delivered to a subscriber’s MNO or handset. See also Message Status.

**Direct Carrier Billing (DCB)**: a payment method allowing consumers to pay for goods, products, support, services and content online on a mobile device, directly via their MNO through their contract or pre-pay account.

**Fraud**: wrongful or criminal deception intended to result in financial or personal gain.

**Fraud Detection Provider**: a company which detects wrongful or criminal deception and implements solutions to prevent fraud.

**Marketing Partner**: [See Affiliate Marketing Partner; Affiliate].

**Marketing Provider**: [See Affiliate Marketing Partner; Affiliate].

**Merchant**: a company which sells goods, products, support, services and/or content online.

**Mobile Network Operator; Mobile Operator; Carrier (MNO)**: An MNO provides wireless or mobile communication services and owns or controls all of the elements of the network infrastructure necessary to deliver services to a mobile subscriber. All MNOs must also own or control access to a radio spectrum license which has been issued by a regulatory or government body. An MNO typically controls provisioning, billing and customer care, marketing and engineering organisations needed to sell, deliver and bill for services, though these systems and functions can be outsourced.
**Mobile Originated (MO)** This describes the source of a sent message, i.e., the beginning of the end-to-end message delivery chain. See also Originating Mobile Operator.

**MSISDN** (Mobile Station International Subscriber Directory Number) The unique mobile phone number attached to a SIM card used in a mobile device.

**Mobile Subscriber, Subscriber, End User** An individual who is a customer of, and connected to, a domestic MNO’s network for services, including voice calls, SMS, MMS, or data.

**Mobile Terminated (MT)** This describes the destination of a sent message, i.e., the end of the end-to-end message delivery chain. See also Terminating Mobile Operator.

**MSISDN Passthrough** When a consumer is on an MNO data connection online within a merchant’s retail environment, the consumer’s MSISDN is passed securely from the MNO to the payment aggregator. The MSISDN is encrypted by the payment aggregator and not revealed to the merchant.

**MVNO (Mobile Virtual Network Operator)** A wireless or mobile communications services provider which does not own the network infrastructure over which it provides services to subscribers. An MVNO will contract with an MNO to obtain bulk access to network services at wholesale rates and then set the retail prices independently. An MVNO may use its own customer service, billing support systems, marketing and sales personnel, or it could engage a third party.

**One-time Password (OTP)** A password which is valid for only one login session or transaction on a device.

**Originating Mobile Operator; Originating MNO** The MNO at the beginning of the end-to-end message delivery chain which accepts messages from a messaging provider for onward delivery.

**Originator** The term used to describe the number or word which identifies who a message is from upon receipt. It is also known as a SenderID. An alphanumeric originator enables a brand name to be set as the identified ‘sender’ of a message.

**Outpayment** A payment made to a contracted party for income generated by a premium rate service, e.g., an MNO makes an outpayment to a payment aggregator and the payment aggregator then makes an outpayment to a merchant.

**Payment Aggregator** A company that provides a payment platform which facilitates mobile payments between MNOs and messaging providers.

**Payment Page(s)** A merchant’s online premium rate retail check-out.

**PRS (Premium Rate Service)** Services which enable mobile subscribers to pay for content, data services and VAS via their mobile phone bill or prepay account.

**PSMS** A payment method which bills consumers via SMS from a charged short code.

**Push Message; Push Notification** A message which pops up on a mobile device via an app.

**Regulator** An organisation or body which exists to establish and maintain a framework within which an industry may operate and which may penalise those who do not operate within the established framework.

**Reseller** A company which buys a product or service, repackages and then sells it as its own.
SDK; Software Development Kit a collection of software development tools in one installable package which can facilitate the creation of applications.

Short Code, Short Number A special number, significantly shorter than a full 11-digit phone number, which can be used to send SMS and MMS messages.

SIM; SIM Card (SubscriberIdentity Module) A smart card inserted into a mobile device which carries a unique identification number, stores personal data and prevents operation of the device if removed.

SMS (Short Message Services) A text messaging service component of phone, web, or mobile communication systems which uses standardised communications protocols to allow fixed line or mobile phone devices to exchange short text messages.

Social Engineering the use of deception to manipulate individuals into revealing confidential or personal information that may be used for fraudulent purposes.

Stakeholder an individual or organisation with an interest or concern in something

Spam A broad term for an unsolicited message, namely, one which is not wanted by the recipient, whether the message has been sent with good intentions or maliciously.

Subscription an arrangement to receive something on an ongoing basis, either regularly or at irregular intervals.
DCB Working Group

This whitepaper was developed by MEF’s DCB Fraud Working Group, a cross-stakeholder global industry group whose goal is to collaborate to raise awareness and provide market education to help build trust and maintain a healthy payments and content ecosystem.
MOBILEECOSYSTEMFORUM.COM

MEF is a global trade body established in 2000 and headquartered in the UK with members across all the world. As the voice of the mobile ecosystem focuses on cross-industry best practices, anti-fraud and monetisation. The Forum provides its members with global and cross-sector platforms for networking, collaboration and advancing industry solutions.

© 2020 Mobile Ecosystem Forum Ltd.
All Rights Reserved.

Disclaimer
Mobile Ecosystem Forum makes no representation, warranty or undertaking with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in these guidelines. The document was developed by MEF’s DCB Fraud Working Group in 2020 and in full compliance with the programme’s antitrust compliance policy. The information contained in this document may be subject to change. Please check for latest version.