WHITE PAPER

Keeping Fraud Away from Mobile Payments

ACHIEVING SUSTAINABLE GROWTH NOT HINDERED BY SCAM TRAFFIC – FOR MERCHANTS AND TELCOS

JULY 2024

Contents

01
GLOBAL MOBILE PAYMENTS MARKET IN A NUTSHELL

02
MOBILE PAYMENT FRAUD IN A NUTSHELL

03
FRAUD ATTEMPTS & DCB PERFORMANCE IN THE MIDDLE EAST

04
HOW TO PREVENT MOBILE PAYMENT FRAUD

Introduction

This report provides insights into the “methods, tips and solutions of preventing fraud” in the mobile payment ecosystem, highlighting the types and dynamics of mobile fraud, various data and evaluations compiled from multiple market research companies.

Over the last 20 years, people have adopted digital lifestyles. They make purchases online, bank over the phone, and even discover new partners with a few clicks and swipes. Mobile payment methods are especially on the rise, even in the financially underserved parts of the globe. Although these methods are becoming more popular options, they still need some time to realise their potentials. However, with the global expansion of mobile payment, fraud techniques are likewise getting more advanced. Actually, fraud is a problem that impacts every stakeholder in the landscape: Telecom operators lose revenue and receive more customer complaints, merchants suffer reputational damage, and end users incur financial losses.

In order to make mobile payment a secure payment procedure, increasing awareness is necessary, as well as robust and comprehensive anti-fraud solutions. In this age of digital monetisation, methods such as direct carrier billing and mobile wallets will prove to be useful instruments for all market participants, particularly Mobile Network Operators (MNOs), to carry out secure everyday transactions. TPAY Mobile, a testament to the effectiveness of DCB, have been working together with cybersecurity specialists for years to prevent fraud against its merchants. This time, we are releasing a TPAY whitepaper to raise awareness about fraud prevention.

Born in Cairo, Egypt, in 2014, TPAY has made it easy for consumers across the Middle East, Türkiye, and Africa (META) to pay for digital services using their mobile devices as the core. The company’s simple but transformative payment technology enables more than 18.6 million monthly active users across 31 countries in the region to make 1.6 billion monthly transactions on its platform.

We improve the META region by delivering cross-border micropayments at scale and significantly improving financial inclusion. As a fintech innovator and mobile technology veteran, this ability to enhance financial inclusion appeals to me more when we do everything fraud-free. I wholeheartedly support the company’s mission of empowering digital economies in the most convenient and secure way.

At TPAY, our market experts have been working intensively on the industry’s significant shifts with various market players. Thanks to their efforts, in this crucial white paper, we take you on a journey of inspiration – but also tangible actions. This paper analyzes the dangers, obstacles, and hazards posed by fraudsters in mobile payment and the methods to mitigate them. Effectively combating fraud is crucial for business success, enabling safe digital monetization and a sustainable mobile ecosystem.

So, without further ado, we invite you to join us on an exciting journey and explore ways of *Keeping Fraud Away from Mobile Payments*!

Işık Uman
CEO, TPAY Mobile

01

GLOBAL MOBILE PAYMENTS MARKET

What are Mobile Payments?

Statista's Digital Market Insights reveals that revenue from mobile e-commerce sales reached an estimated 1.7 trillion USD[1] in 2023, accounting for the majority of all retail e-commerce sales. Globally, a large part of e-commerce growth is driven by consumers using their mobile devices, phones and tablets to acquire goods and services. The share of mobile e-commerce in all e-commerce has been on a steady climb, up from just 52% in 2022 to an expected 63% in 2028.

The definition of mobile payment is quite clear: A mobile payment is a transaction conducted and completed using a mobile device -such as a smartphone, a tablet, or even a smartwatch- and a payment instrument like a bank account or debit/credit card, transport card, gift card, or a mobile wallet like PayPal or Direct Carrier Billing. With this payment method, consumers do not need to take out their wallets or credit cards to purchase goods or services from a business or simply to send money to each other. Consumers pay for services from their smartphones, transferring money between accounts, or moving money from one account to another. These payments can be made using digital wallets or peer-to-peer platforms. Mobile payment is a lot of things: It is e-commerce on a smartphone, payment via the phone bill (Direct Carrier Billing -DCB), mobile POS, airtime payment and more.

For consumers, mobile payment offers a safe alternative to cash-based transactions and allows for rapid money transfers. In some countries, mobile payment methods are the most frequently used, with the highest proportion of users leveraging them at least weekly.

Some mobile payment types such as digital wallets and peer-to-peer payment apps have been popular for years, but their popularity skyrocketed in 2020 due to COVID-19 and pandemic lockdowns. According to a Mastercard's survey[2], 79% of respondents worldwide say they used contactless payments amid the COVID-19 pandemic, citing safety and cleanliness as key drivers.

[1] *"Mobile Commerce Revenue and Share of Total Retail E-commerce Worldwide from 2017 to 2028," Statista, April 30, 2024 - https://www.statista.com/statistics/1449284/retail-mobile-commerce-revenue-worldwide/*

[2] *"Consumers Globally Make the Move to Contactless Payments for Everyday Purchases," Mastercard Press Release, April 29, 2020 - https://www.mastercard.com/news/press/press-releases/2020/april/mastercard-study-shows-consumers-globally-make-the-move-to-contactless-payments-for-everyday-purchases-seeking-touch-free-payment-experiences/*

Digital wallets are financial applications that allow you to store funds, make transactions, and track payment histories on smartphones and tablets. Some digital wallets also allow users to send money between individuals, meaning a small business contractor or service provider can receive money directly. Convenience and speed of money transfers still play a large part in their rising popularity.

On the other hand, peer-to-peer payments allow individuals to send and receive money directly, which is convenient and fast. They, too, simplify transactions.

Basic Forms of Mobile Payments

The term "mobile payment" actually describes many different financial transaction activities facilitated through or on a mobile device. As such it includes:

Using a phone to pay for something on a mobile website or an app; sending money to a friend from a mobile wallet; using a phone to pay for something in a shop – using a contactless tap or barcode scan; paying for goods and services using phone credit; paying for goods and services using a dedicated mobile money account. Together, these mobile payment scenarios that have a rich history of driving innovation create an ecosystem space that handles trillions of dollars, supports the income of millions of global citizens and has a rich history of driving innovation.

If we categorize all these activities under distinct groups, the basic forms of mobile payments are proximity payment and remote payment.

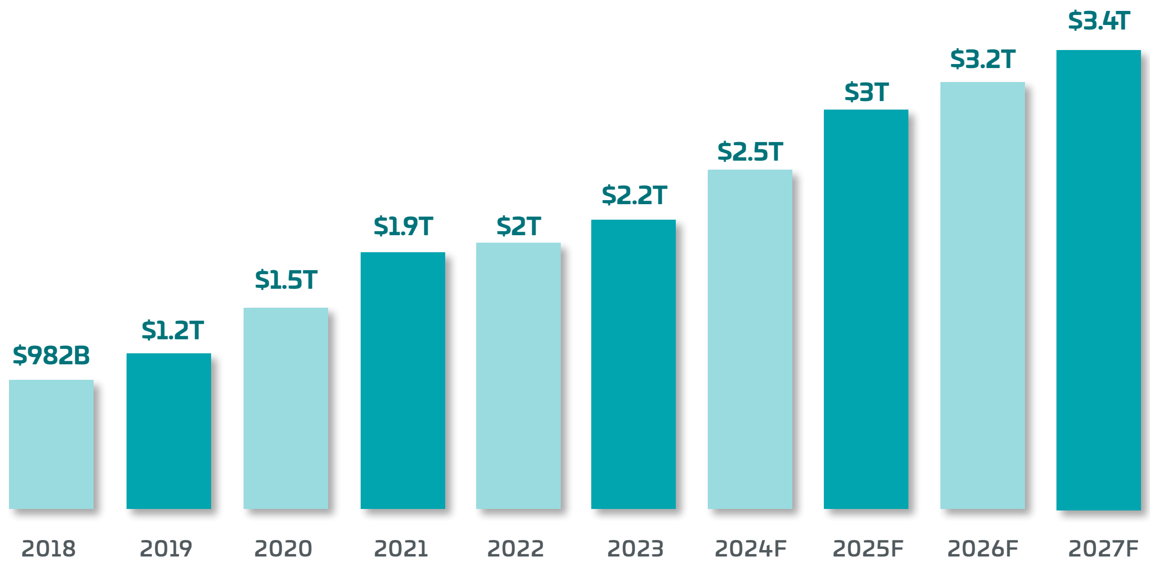
Proximity payment: This refers to in-store payment solutions using smartphones. This market is exhibiting rapid growth owing to its instant payment offerings. The proximity payment segment of mobile payments is further sub-segmented into Near-field communication (NFC) and QR code payments.

NFC payments are a form of contactless payment that uses near-field communication technology, that wirelessly transfers data during a purchase via a smartphone or tablet by sharing it with another device.

QR code payment is a contactless method in which consumers scan a QR code from a mobile app to be directed to a payment page. It is becoming increasingly more common in the payment processing landscape. QR code payment contains encoded data in a unique pattern of black-and-white squares and is convenient for both online and offline payments.

App-based mobile payment is another form of contactless payment. Some merchants, particularly food giants like Starbucks and McDonald's, have their own apps that customers can use to pay. Combining the convenience and safety aspects of contactless payment via a mobile phone or other devices, app-based mobile payment lets consumers

Figure 1: Global Mobile E-commerce Sales by Year



F = forecast

Source: Statista Market Insights, 2023 buy goods or services directly via the merchant's app.

Remote payment: Remote payments do not require any direct interaction. They offer the ease of contactless payment through the available real-time online terminal. This payment segment is further categorised into browser-based mobile (internet) payments, direct carrier billing, digital wallets, and linked-based (SMS) payments.

Browser-based transactions mean users purchasing online via their smartphone or tablet. The customer enters their payment information into the website checkout form and pays depending on what the merchant offers.

Direct Carrier Billing (DCB) is a type of online payment that allows consumers to charge the cost of a purchase to their mobile phone bill.

Digital wallets like Apple Pay, Google Pay, PayPal, and Samsung Pay allow users to store their debit, credit, and gift cards or bank accounts within a mobile phone. Once linked, purchases can be made using a mobile smart device rather than a physical card—both online and in-store at retailers that have NFC receivers.

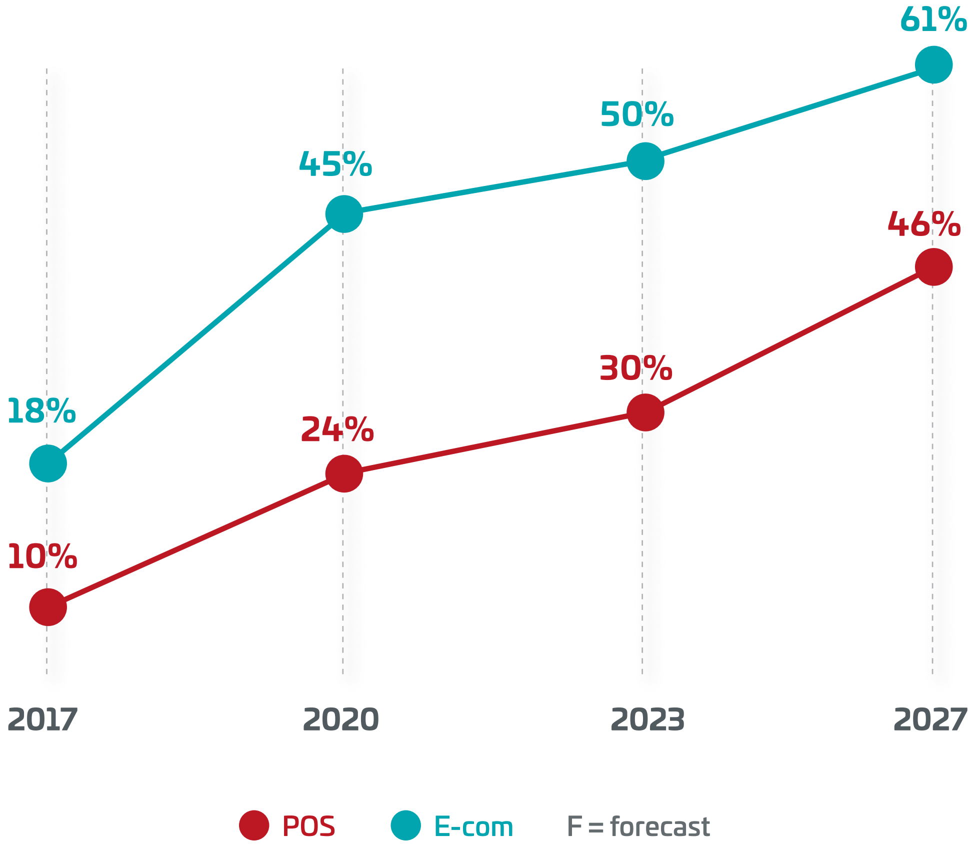
Link-based payments or SMS payments are processes initiated by merchants sharing with consumers a URL as a mobile message, which functions similarly to QR codes. As a quick and convenient way for merchants to get paid by their customers, payment links—sometimes called pay by link—direct consumers to a secure checkout page, where they can make a purchase after entering their payment details. By accepting payments across multiple channels, payment links allow merchants to address cart abandonment issues and increase conversion rates directly.

Global Mobile Payment Market

Changing technologies have significantly impacted the global payments landscape throughout history. Cash in all its forms dominated for millennia and through the industrial age. Once information was encoded in analogue electronics in the 20th century, we witnessed the reign of plastic cards. Thanks to the development of the World Wide Web and electronic commerce, alternative payment methods flourished in the late 1990s. A wide variety of

Figure 2: Digital Wallets Share of Global Transaction

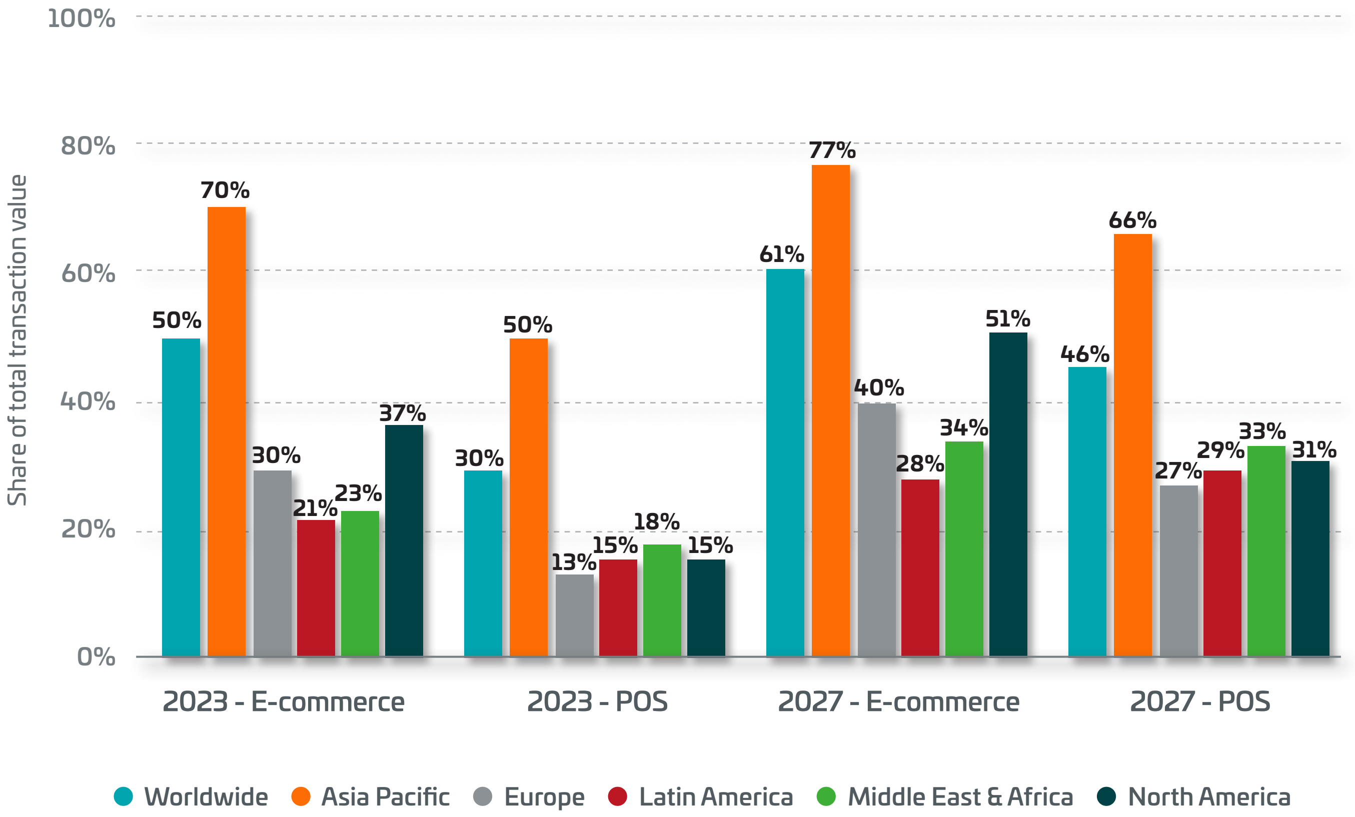
Value % 2017-2027F



Source: "Global Payments Report 2024", p. 12, WorldPay, 2024

Figure 3: Global Market Share of Mobile Wallets

In e-commerce and POS in 2023 with 2027 forecast



Source: "Market Share of Digital/Mobile Wallets in Total E-commerce and POS Transaction Value Worldwide in 2023 with a Forecast for 2027, by Region," Statista, March 2024

payment choices are now produced by digital technologies, with the market for mobile payment options rising at the highest rate.

Fortune Business Insights, a customer research and consultancy company, explains in its report, "Mobile Payment Market Forecast, 2024-2032," that the market is expected[3] to exhibit a CAGR of 28.1% during the forecast period of 2024-2028. Digitalization of payment services and rising e-commerce businesses are said to be the main factors driving the market's development.

Asia Pacific accounts for the largest global mobile payment market share. Leading the globe with around 46% in 2022, Asia Pacific owed its dominant position in driving the mobile payment market growth to mainly government initiatives. These initiatives facilitate convenient transactions but also contribute significantly to fostering a more efficient and secure financial ecosystem across the region.

Among the various forms of mobile payments, digital or mobile wallets seem to grow the fastest throughout the world. A payment technology and solutions company, Worldpay's "Global Payments Report, 2024"[4] showed that digital wallets are the major payment method online, executing 50% of global e-com transaction value in 2023. In their ninth edition of The Global Payments Report, Worldpay offers a snapshot of today's consumer-to-business payments landscape: globally, by region and in 40 selected markets that account for 88% of global GDP. According to the 2024 report, wallets accounted for 30% of global POS spend, or more than 10.8 trillion USD.

Still the fastest-growing payment method, wallets are projected to account for more than $25 trillion in global transaction value (49%) across e-commerce and POS by 2027.

Emerging countries use digital wallets as a driver to reach their financially underserved or unbanked

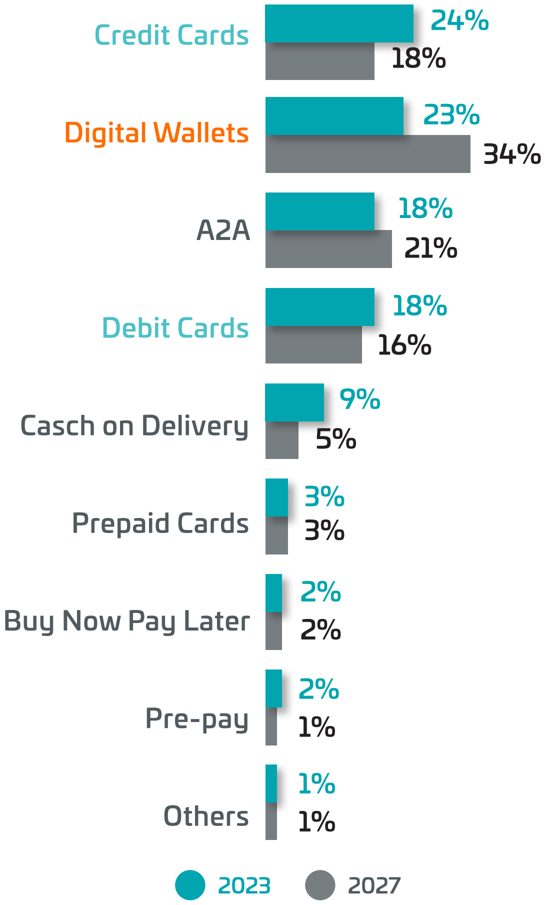
[3] *"Mobile Payment Market Size, Share & Industry Analysis and Regional Forecast, 2024-2032," Fortune Business Insight, 2023 - https://www.fortunebusinessinsights.com/industry-reports/mobile-payment-market-100336*

[4] *"Global Payments Report 2024", p. 10, WorldPay, 2024 - https://worldpay.globalpaymentsreport.com/*

population. That's why digital wallets are projected to become the leading POS payment method in Latin America, Middle East & Africa by 2027.

Figure 4: MEA E-com Payment Methods

Transaction value % 2023-2027F



2023 = estimate, 2027 = forecast

Source: "Global Payments Report 2024", p. 134, WorldPay, 2024

Payment Methods in MEA

E-commerce Payments: In terms of e-commerce transaction value as a percentage of all commerce (including e-commerce and POS sales), Middle East and Africa (MEA) considered among the top. Global e-commerce (e-com) sales represented approximately 14% of all commerce in 2023. By 2027, e-commerce is expected to account for 17% of global commerce, with higher growth rates compared to POS.

Credit cards maintained a general lead in e-com payments across MEA in 2023 representing 24% of regional online spending. Both credit cards and debit cards are expected to expand in transaction value in all four MEA markets through 2027, although at slower rates than digital payment methods, resulting in a steady loss of share.

Digital wallets are the fastest-growing online payment method globally and also in MEA. According to Worldpay data, wallets continue to dominate e-commerce, accounting for 50% of global transaction value in 2023. In MEA, wallets accounted for 23% of regional e-commerce expenditure in 2023, with transaction value increasing by 35% annually. By 2027, wallets are expected to account for 34% of e-commerce value, growing at a 26% CAGR.

Four MEA markets covered for the Worldpay study (Saudi Arabia, UAE, Nigeria, and South Africa) represent the highest use of cash on delivery among all global regions at 9% of 2023 regional online spending, followed by having the highest regional use of cash overall.

Account-to-account (A2A) payments are forecasted to see tailwinds from new real-time payment rails as well as efforts to establish interoperability

> DCB has emerged for both merchants and consumers as a fast and convenient payment method. Because DCB only needs an active mobile number to deduct the purchase amount from the credit balance or add it to its monthly bill, it is gaining ground, especially in financially underserved regions worldwide.

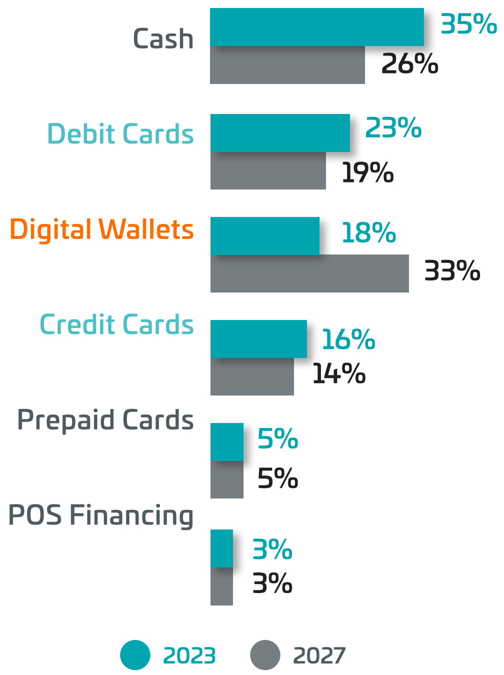
between domestic schemes across the region. Accounted for 18% of regional e-com spending in 2023, A2A transaction values across the region are projected at 17% CAGR through 2027.

POS Payments: Point of sale (POS) payments consist of business-to-consumer transactions which occur at a physical location "point of sale." According to Worldpay analysis that includes traditional in-store transactions as well as all face-to-face transactions, digital wallets continue their phenomenal growth regardless of where they take place. Mobile money-stored value wallets such as e& money, M-PESA, MTN MoMo, and Orange Money are popular in the region, and many are historically able to execute payments by text with feature phones. They compete with super apps like Vodapay, pass-through wallets such as stc pay in Saudi Arabia, Apple Pay and Google Pay across the region. In 2023, wallets accounted for 18% of POS transaction value. By 2027, they are expected to account for 33% of POS spending across the four MEA markets at a 21% CAGR, as highlighted in the Worldpay report.

On the other hand, cash remains the leading payment method, accounting for an estimated 35% of POS transaction value across the four MEA markets (Saudi Arabia, UAE, Nigeria, and South Africa) covered in the GPR 2024 of Worldpay. While the highest in any region, cash use in these markets is forecasted to still register 26% of POS transaction value in 2027.

Figure 5: MEA POS Payment Methods

Transaction value % 2023-2027F



2023 = estimate, 2027 = forecast

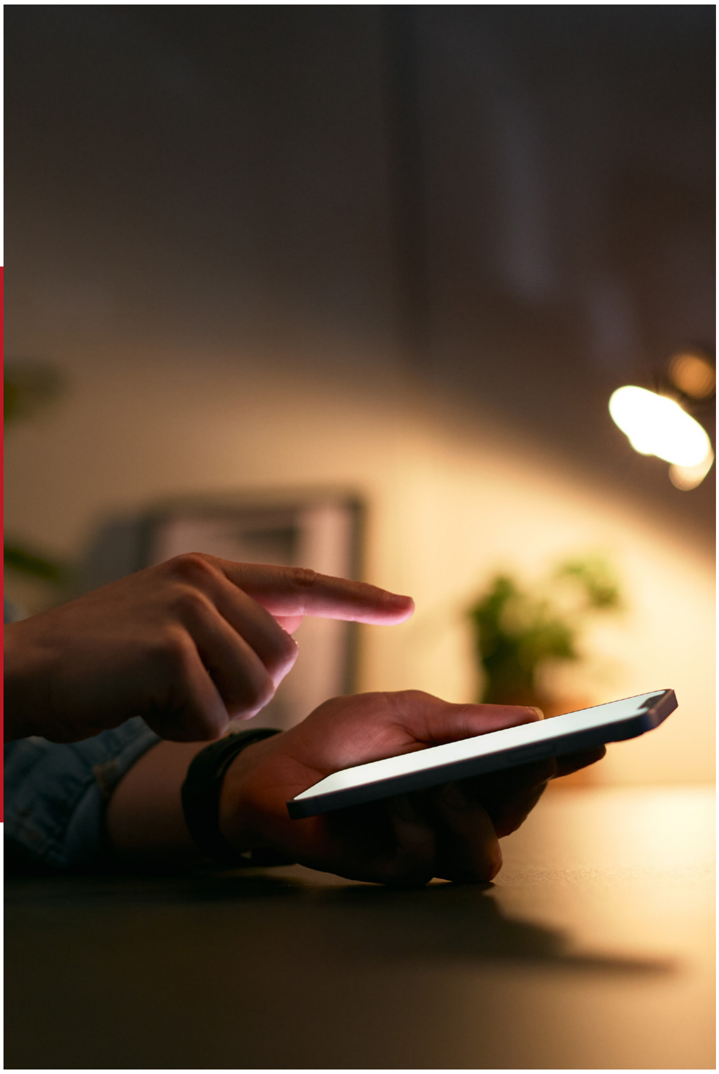
Source: "Global Payments Report 2024", p. 136, WorldPay, 2024

DCB as the Most Convenient Method

As an uncategorized e-commerce payment method, direct carrier billing (DCB) is accepted as the most prominent mean of online transactions among the unbanked population of the Middle East and Africa. Also known as "operator billing," DCB has emerged for both merchants and consumers as a fast and convenient payment method that is rapidly gaining popularity. Because all it needs is an active mobile number to process the transaction and pay it via the mobile number, DCB finds its foothold, especially among the financially underserved regions. People with a pre-paid plan can simply top up and begin making a purchase. For post-paid subscribers, it could also be the most convenient source of credit with a sort of "buy now pay later" plan as the carrier's monthly bill.

With a large percentage of the population owning mobile phones, the MEA region is one of the fastest-growing DCB markets in terms of mobile connections. DCB is a pure telco payment option that allows mobile phone owners to pay for online goods, products, and services (digital or otherwise). DCB market is experiencing a remarkable surge in growth, driven also by the increase in demand

> Not only do businesses lose money on transactions, but fraud can also affect brand reputation and customer loyalty. If telcos, payment aggregators, and merchants wish to increase customer trust and loyalty, they should integrate some form of anti-fraud solutions into their payment systems.



for games, video-on-demand services, eBooks, podcasts, and other digital content.

The global Direct Carrier Billing Platform market was valued at 46,74 billion USD[5] in 2023 and is anticipated to reach 155,28 billion USD by 2030, witnessing a CAGR of 18.4% during the forecast period 2024-2030.

The major global companies offering DCB Platforms include Bango, Boku, Centili, Comviva, Digital Turbine, Digital Virgo, Dimoco, Fortumo, NTT Docomo, Singtel.

It is anticipated that DCB will play an increasingly important role in the future of digital payments as the global payment ecosystem continues to evolve. Because it is deemed to be a seamless and secure payment method. DCB is secure because users are required to confirm the payment on their physical devices. The fact that the user does not need to reveal personal data during the payment process makes DCB a secure payment method.

Mobile Payments' Non-immunity

For many financial institutions, offering convenient and safe mobile payment methods such as DCB gives them a competitive advantage. However, even DCB transactions are not totally immune to the risk of fraud, which can be extremely costly for businesses. Although rapid technological advancements have accelerated innovation in mobile payment methods, they've also created vulnerabilities that fraudsters can easily exploit. Not only do businesses lose money on transactions, but fraud can also affect brand reputation and customer loyalty.

If telcos, payment aggregators, and merchants wish to increase customer trust and loyalty, they should integrate some form of anti-fraud solutions into their payment systems to safeguard their transactions. Before getting into the details of fraud prevention strategies and tackling mobile fraud detection, it's important to understand how cybercriminals mimic the users who make payments from their mobile devices. So, let's dwell briefly on mobile payment fraud and its types in the coming chapter.

[5] *"Global Direct Carrier Billing Platform Market Research Report 2024," Absolute Reports, February 2024 - https://www.absolutereports.com/global-direct-carrier-billing-platform-market-26741306*

02

MOBILE PAYMENT FRAUD IN A NUTSHELL

What is Mobile Payment Fraud?

The Association of Certified Fraud Examiners (ACFE), the world's leading anti-fraud body, defines[6] fraud as any activity that relies on deception in order to achieve a gain. Fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment".

Mobile payment fraud is defined as any fraudulent or unauthorized behavior that causes challenges for players who are not adequately safeguarded throughout a transaction. Mobile payment fraud involves any dishonest or malicious actions intended to take advantage of vulnerabilities in mobile payment systems or trick users into giving up access to their financial accounts or personal data.

According to McKinsey, the global payment industry is exceeding pre-pandemic expectations, topping 3 trillion USD[7] by 2026, and registering double-digit gains each year. This is attracting top telco players around the world who are making sure they take advantage of this opportunity.

But so are cybercriminals and fraudsters. Then, the question is how costly online fraud is? It's very costly. As shown by Juniper Research, the foremost experts in payment markets, merchants lost around 38 billion USD to online fraud in 2023 alone, and these figures will rise to 91 billion USD by 2028. Their report titled "Online Payment Fraud: Market Forecasts, Emerging Threats & Segment Analysis 2023-2028"[8] says that merchant losses from online payment fraud combined will exceed 362 billion USD globally between 2023 and 2028. Juniper Research report demonstrates that the rise in e-commerce transactions in emerging markets is driving this growth. Merchants there face new threats, such as an increased use of AI for attacks.

Senior Research analyst at Juniper and the author of the report Cara Malone underlies the importance of awareness and education with her remarks[9]: "Fraud detection and prevention providers must educate their clients in the importance of data sharing, in order for the highest accuracy within their solutions. This is increasingly important with the growing use of AI, as it utilises a variety of data to examine patterns within fraud, which is extremely advantageous in a space where fraudsters usually attack at scale, rather than attacking a specific customer."

Outseer, the global leader in payments authentication and monitoring solutions, demonstrates in its latest "Outseer Fraud & Payments Report: 1H 2022," that 70% of fraudulent transactions occur within the mobile channel[10]. The analysis report of fraud attacks and consumer

[6] *Association of Certified Fraud Examiners (ACFE), 2023 - https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud*

[7] *"The 2022 McKinsey Global Payments Report," p.5, McKinsey & Company, October 2022 - https://www.mckinsey.com/industries/financial-services/our-insights/the-2022-mckinsey-global*

[8] *"Online Payment Fraud: Market Forecasts, Emerging Threats & Segment Analysis 2023-2028," Juniper Research, June 2023 - https://www.juniperresearch.com/research/fintech-payments/fraud-identity/online-payment-fraud-research-report/*

[9] *"Losses from Online Payment Fraud to Exceed $362 Billion Globally Over Next 5 Years," Juniper Research Press Release, June 26, 2023 - https://www.juniperresearch.com/press/losses-online-payment-fraud-exceed-362-billion/*

fraud data collected by the Outseer Research team from the first half of 2022 also shows that 75% of fraudulent online banking payments activities originate from trusted accounts on trusted devices. This suggests that consumers are unwittingly parting ways with their money, having been duped by fraudsters' scams.

Another finding of the report is that the growth of card-not-present (CNP) digital payments continues to rise, bringing with it the increased risk of fraud and the majority of CNP fraud that was observed was based upon account takeover.

A rise in e-commerce transactions in emerging markets is also driving this growth. Merchants there face new threats, such as increased use of AI for attacks. Increasing losses in the industry highlight the importance of robust security features for mobile payments.

Global Dynamics & Types of Fraud

Although merchants can profit greatly from accepting mobile payments, thus increasing their revenues, there are certain risks attached as well. Cybercriminals take several approaches to payment fraud depending on their objectives, their capacity to obtain the required information, and the potential financial exploitation. Thus, there is no single threat vector. The environment of fraud is intricate and multifaceted; fraudsters' methods, strategies, and instruments vary from country to country and industry to industry. Fraudulent actors use a range of tactics to get access to sensitive payment information or carry out unauthorized transactions. However, they do not usually know which tactic will work when they attack a certain target. So, they usually try multiple methods until they find the vulnerability they want.

So, mobile payment fraud takes several forms, such as identity theft, account takeover, synthetic identity fraud, and friendly fraud, etc.

Identity theft: The ultimate objective is to sell personally identifiable information (PII) on darknet marketplaces or use it to open fraudulent financial accounts and thereafter make the transaction. PII can be taken through social engineering, phishing, or business resources. According to the "Identity Fraud Report 2024,"[11] compiled by Veriff, 6% of all verification attempts were fraudulent in 2023. Identity fraud itself was the biggest threat, at an average of 6.03% over the course of 2023.

Account takeover: Users may give their login credentials to cybercriminals using phishing and social engineering techniques, or they may have their login credentials stolen from a third-party data breach and use them across several online accounts, leaving those accounts vulnerable to a hijack. Any type of online account – banking,

[10] *"Outseer Fraud & Payments Report: 1H 2022," Outseer Research Team, September 2022 - https://www.outseer.com/fraud-report-2022-h1/*

[11] *"Identity Fraud Report 2024," Veriff 2023 - https://www.veriff.com/ebooks/veriff-fraud-report-2024*

> The most common types of online payment fraud that will affect merchants in 2024 include account takeover, friendly fraud/chargeback abuse, synthetic identity theft, promo abuse, e-gift card fraud, affiliate fraud, and triangulation fraud.

credit, e-commerce, brokerage, reward points, social security, healthcare or social media – can fall victim to account takeover fraud. As a lesser-used but effective form of fraud, account takeover (ATO) fraud is projected to become more popular as cybercriminals look for ways to escape current anti-fraud measures and deceive victims.

Synthetic identity fraud: Financial accounts that may be connected to a particular person are created using a mix of true identity data and faked information. By fabricating recent births or using homeless citizens' IDs or social security numbers in an analogue way, first fraudsters cobbled together dozens of fake people for use in their mortgage fraud scheme. The digital creation of synthetic identities is now one of the top fraud trends. Synthetic fraud hits the financial sector the hardest, and it's the fastest-growing fraud type in that sector.

Friendly fraud: By taking advantage of weaknesses in corporate processes or application vulnerabilities, legitimate customers can fraudulently obtain reimbursements from chargebacks. Sometimes referred to as "chargeback fraud", friendly fraud can be accidental. But sometimes it's done intentionally by criminals, who place orders and claim they never received them. Unfortunately, the person committing this type of fraud is virtually indistinguishable from the regular customers.

Card-Not-Present (CNP) fraud: CNP fraud is the most common type of mobile payment fraud. It happens when someone with malicious intent gets hold of crucial payment details, such as credit card numbers, personal information (cardholder's name, billing address, etc.) or the three-digit CVV security code and link this information with a new mobile device. Once the fraudster has stolen these details, then he can make fraudulent purchases; and the transaction may appear legitimate. CNP fraud can also be committed by getting a lost or stolen mobile device and using its mobile wallet to make unauthorized purchases with it, either online or in-store.

In a market analysis released by Ekata[12], a global leader in dynamic identity verification solutions for real-time risk decisioning, the most common types of online payment fraud that will affect merchants in 2024 include account takeover, friendly fraud/chargeback abuse, synthetic identity theft, promo abuse, e-gift card fraud, affiliate fraud, and triangulation fraud.

According to another report, conducted by MRC on Global Payments & Fraud, the most prevalent types of e-commerce fraud in 2023 were chargebacks, refund abuse/coupon abuse, account reactivation, identity theft, and card testing. At the same time, about 85% of merchants have already started implementing Strong Customer Authentication (SCA) to comply with the EU's PSD2 and PSD3 regulations. "Even so, the process is cumbersome and adds complexity to how merchants manage compliance and how they navigate fraud and payments,"[13] thinks Irina Ionescu, senior editor of the Paypers report in her foreword column.

On the other hand, The Merchant Risk Council's (MRC) 2024 report, based on the findings of the "2024 Global eCommerce Payments & Fraud Survey 2024,"[14] delivers valuable insights gathered from a global survey of more than 1,100 merchants from over 35 countries across North America, Europe, Asia-Pacific (APAC), and

[12] *"5 Best Practices to Preventing E-commerce Fraud in 2024," Ekata blog site, January 10, 2024 - https://ekata.com/resource/5-industry-best-practices-to-preventing-ecommerce-fraud-in-2024-2/*

[13] *"Fraud Prevention in Ecommerce Report 2023-2024," p. 3, Paypers, 2023 - https://thepaypers.com/reports/fraud-prevention-in-ecommerce-report-2023-2024/r1265410*

[14] *"The 2024 Global eCommerce Payments & Fraud Report," The Merchant Risk Council (MRC), p.7, 2023 - https://info.merchantriskcouncil.org/hubfs/Reports/Fraud%20Reports/2024_Global_Payments_and_Fraud_Report.pdf*

Latin America (LATAM) regions. Here are just some highlights:

- Merchants accept 4.6 different payment methods on average. Globally, roughly three-quarters of eCommerce merchants accept cards and digital wallet payments, and most also take debit transfers and mobile payments.
- 8 out of 10 (82%) merchants began accepting at least one new payment method over the past year. Real-time payments (RTP) and buy now, pay later (BNPL) are among the fastest-growing acceptance methods, along with digital wallets, debit transfers, and mobile payments.
- Card and digital wallet payments, followed by mobile payments and debit transfers are perceived as having the highest fraud rates, even though they are the most widely accepted.
- 9 out of 10 merchants encourage customers to pay via certain, preferred payment methods, usually by prioritizing or promoting these methods at checkout. Merchants are adopting this, in the objective of reducing fraud and minimizing processing costs.
- More than 90% of merchants employ at least one tool or technique designed to boost payment authorization rates, for instance, automated retries or intelligent payment routing. Merchants are increasingly making use of third-party data to improve the effectiveness of authorization-boosting tactics.

When it comes to tools and techniques merchants employ to monitor and prevent fraud, the 2024 'Global eCommerce Payments & Fraud Report' focuses on tools driven by AI and/or ML. As shown in the figure below, the adoption of these fraud management tools is likely to grow swiftly over the coming months and be implemented and integrated into merchants' IT systems worldwide.

A Mobile Payment Scam Example

With mobile payment scams, scammers may attempt to trick you into sending them money through a mobile payment method like PayPal. That's because they know it's hard for you to get your money back once you do. If you link such services to your bank account or debit card, it's almost like handing someone cash. So, be aware of how this scam works. The following is an overview of the scam:

1. A Middle Eastern Bank customer receives an SMS that looks like a fraud alert from the bank. The message may say, "Did you make a purchase of $750.50 at ABC Store?".

2. When the customer responds "No" (because the text was bait), the scammer will respond that someone from that Middle Eastern Bank will contact you.

3. They will then call the customer. In many cases, the number they are calling from appears to be the bank's actual phone number, which they have spoofed. (Caller ID is not a reliable source for identifying callers.) The scammer will proceed to offer to help with the customer's fraudulent activity. They will ask for a one-time code you would have received via text from "the bank." (Remember, while banks may send text messages to validate unusual activity on your account, they will NEVER ask you to share a security code or your online banking credentials to resolve fraud!)

4. If the code is given to them, they will use it to enroll their bank account with the mobile payment app using your contact information or something that may resemble it. They may even have you change and share your online banking credentials. (Remember, Banks never ask for this!)

5. If successful, the scammer can now access your account via the mobile payment app. And if a customer shares their online banking credentials, many more kinds of fraudulent transactions can occur.

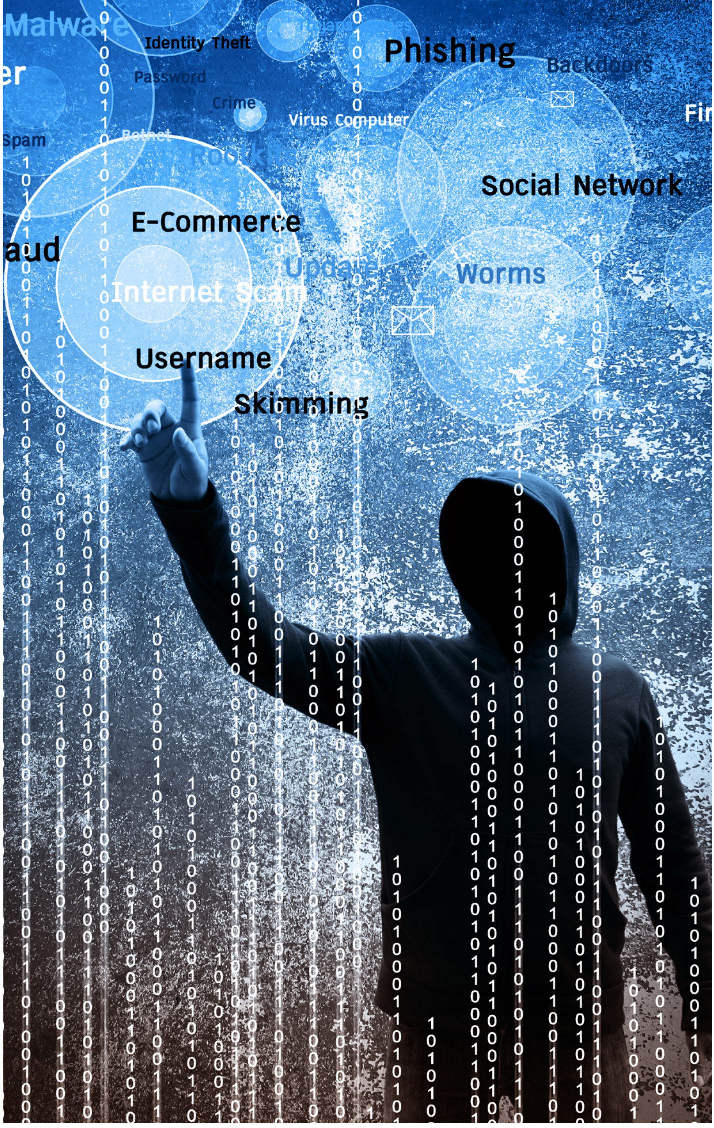
Types of DCB Fraud in General

DCB is fast and convenient for both merchants and consumers. However, DCB is no exception. There is always the risk of fraud, if there are digital transactions involved. It goes without saying that dishonest people and criminal networks target the DCB payment method in an effort to scam consumers, MNOs, payment aggregators, and mobile content providers.

Fraudsters use these attributes for two major purposes. First, they deceive clients into making unnecessary purchases by using social engineering. A more technical form of manipulation is the second. Here, scammers take advantage of technology—bots, click farms, etc.—to obtain fraudulent payouts from companies promoting or endorsing DCB-enabled services.

Fraudsters target all links in the mobile content value chain. The various players in the value chain have different exposure to risks and contrasting incentives. However, every stakeholder is affected. Here is how DCB stakeholders are impacted by fraud:

- Consumers lose money when they are tricked into making unwanted purchases, and they lose trust in the channel and the MNO.
- Merchants lose revenue when de-frauded consumers churn. They face fines, suspensions or service cuts by the affected Mobile Network Operators (MNOs) and by regulators. Also, their brand reputation is impacted negatively.
- DCB payment aggregators might have no control over incoming traffic but will pay a high price if the traffic comes from fraudsters. They might damage their relationships with carriers and regulatory bodies. Lack of trust negatively impacts business.
- DCB fraud detection providers “benefit” from fraud in a sense. They must be careful never to be seen to perpetuate it.
- MNOs suffer from DCB fraud at every turn. Their customer service calls increase, they might lose unhappy subscribers, and their brand's reputation is damaged.



One of the leading fighters against DCB fraud is Mobile Ecosystem Forum Ltd. (MEF). As an independent authority in the mobile industry with members in 45 countries, MEF’s DCB Fraud Working Group published its “Anti-Fraud Yearbook 2023,”[15] late in 2023. In it, MEF explains two main forms of DCB fraud, as a general distinction:

DCB ad fraud: A large percentage of DCB fraud targets the advertisements that VAS businesses conduct. These companies place adverts on mobile sites. Then, using a number of techniques, fraudsters create payouts for clicks. When the user clicks on a link, all the steps of the payment flow are clicked upon automatically. This type of fraud is, not exclusive to DCB. It is the same as any other ad-based mobile fraud.

Consumer-targeted DCB fraud: Essentially, fraudster uses social engineering and/or deception to trick DCB consumers into making unintended purchases – or signing up for unwanted subscriptions. Here are the main types:

[15] *“MEF Anti-Fraud Yearbook 2023,” Mobile Ecosystem Forum Ltd., 2023 - https://mobileecosystemforum.com/mef-anti-fraud-yearbook-2023/*

> Both large and small organizations are significantly impacted by these crimes. Additionally, fraud is not limited to a single industry. Any industry is susceptible to payment fraud, but some are more vulnerable than others. Here are the most affected industries:

A. Misinformation: In this case, the merchant gives all the data that authorities require. They distort or leave out important details, though. A few examples of the techniques employed are:

- Extremely tiny or unreadable price details
- An excessive focus on free trials
- Payment triggering calls to action of a misleading kind, such as "Play Now" or "Get It Here."

B. Disinformation: In this case, the fraudster gives false information, omits it completely, or distorts it. In addition, they conceal billing receipts, making it hard for customers to cancel a fraudulent subscription.

C. Misleading incentives: It is a phishing type of scam. Here, the customer reacts to a promotion like "You have won a prize!" or "A virus has been found on your device." Once the activity is performed, the fraudster deceives the user into taking additional actions that result in an unplanned purchase.

D. Trust manipulation: Another kind of phishing. This time, the fraudsters pose as a close friend or a reputable company. For instance, they might use the typeface, colours, and logo of an authentic brand to create a link to a fake shopping page. These messages can occasionally originate from a contact whose account has been hacked.

What Industries Are Most at Risk

Fraudulent transfers to or from a platform are the most common type of platform fraud, comprising over three-quarters of all incidents. Even though economic and financial crimes' rates are steady, both large and small organizations are significantly impacted by these crimes. Additionally, they are not limited to a single industry. Any industry is susceptible to payment fraud, but some are more vulnerable than others. According to a Stripe resource[16], here are the most affected industries:

Retail: Retail businesses are often targeted by fraudulent actors due to the high volume of credit card transactions and the ease of access to credit card information. Online retailers, which are particularly vulnerable to payment fraud face financial losses, reputational damage, and legal liabilities as a consequence, as fraudulent actors can use stolen credit card information to make fraudulent purchases from anywhere in the world.

Banking and finance: Banks and other financial institutions are prime targets of payment fraud due to the sensitive nature of the information they hold. Fraudulent actors employ sophisticated strategies to steal customer information or use social engineering techniques like phishing to gain access to accounts and engage in illicit transactions.

Healthcare: Healthcare providers are often targeted by fraudulent actors due to the sensitive nature of patient data. Fraudulent actors may attempt to steal patient information or use fraudulent billing schemes to obtain payments.

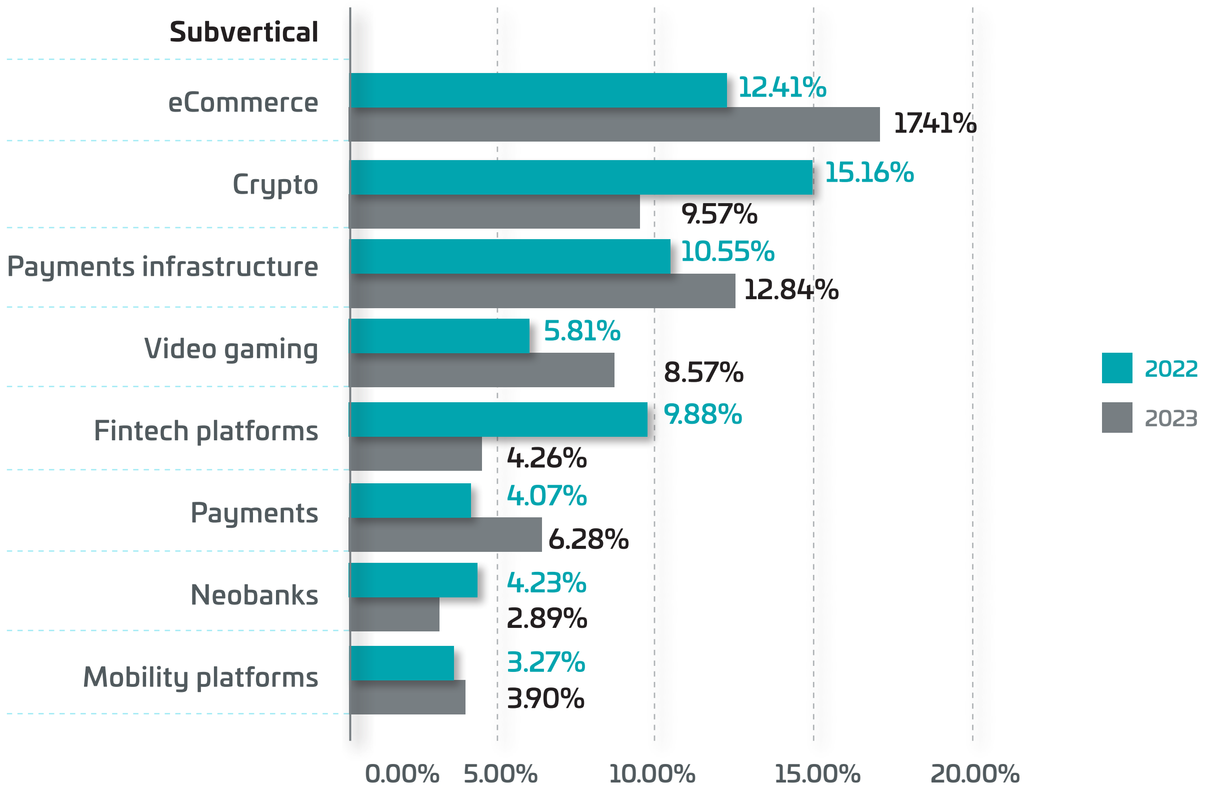
Hospitality: The hospitality industry is at risk of payment fraud through various channels, including online bookings, reservations, and point-of-sale transactions. Fraudulent actors may attempt to steal credit card information or use stolen credit cards to make fraudulent purchases.

E-commerce: E-commerce businesses are vulnerable to payment fraud due to the ease of access to credit card information and the frequency of card-not-present transactions. The digital nature

[16] *"Payment Fraud 101: How It Works and How to Protect Your Business," Stripe, October 16, 2023 - https://stripe.com/resources/more/payment-fraud-101*

Figure 6: Fraud Rate Comparison for Verticals

Annual mean for 2022 vs 2023



Source: Identity Fraud Report 2024, Veriff

of e-commerce poses a challenge in verifying the identity of buyers. and the anonymity of online purchases. Fraudulent actors may use stolen credit card information to make fraudulent purchases or set up fake online stores to obtain payments.

The fact is there is no single story in online fraud across the industries, which range from gaming to financial services. According to Veriff's "Identity Fraud Report 2024,"[17] compiled after extensive analysis of global customers data throughout 2023, identity fraud accounted for 93% of total financial services fraud. However, 77% was authorized fraud - fraud where the victim is deceived into authorizing a transaction. In financial services, it is far greater than any other industry. The graph on this page illustrates how the fraud rate comparison for verticals changed within the last couple of years.

How Does Mobile Payment Fraud Affect Businesses?

The impact of payment fraud can have severe consequences for businesses, financial institutions and individuals. Most importantly, ongoing fraud concerns may lead to a reluctance to adopt new payment technologies and innovations, hindering progress in the financial sector. Here are some other key aspects of the impact[18]:

Financial loss: Payment fraud results in direct financial losses for businesses who may have funds stolen from their accounts or unauthorized transactions made on their behalf. If a fraudulent actor is able to steal funds or goods from a business, the business may have to absorb the cost or pass it on to customers, which can harm the bottom line. Complaint management has also a high

[17] *"Identity Fraud Report 2024, Veriff - https://www.veriff.com/ebooks/veriff-fraud-report-2024*

[18] *"Payment Fraud 101: How It Works and How to Protect Your Business," Stripe, October 16, 2023 - https://stripe.com/resources/more/payment-fraud-101*

cost in terms of time and money. Fraud can also hurt customer retention and decrease customer lifetime value (LTV).

Reputational damage: Fraud is the major unaddressed culprit of damages to the brand image. Beyond hurting the LTV of individual customers, fraud can tarnish a business's reputation and create panic amongst the network's consumers, potentially leading to a loss of customer loyalty. Customers may believe they are untrustworthy or insecure. This can lead to a long-term loss of customers and revenue. MNOs are hindered from becoming major players in mobile payment field.

Legal and regulatory consequences: Financial institutions and businesses have a legal and regulatory obligation to be diligent about fraud prevention; failing to comply with data protection and security regulations may result in potential fines. Payment fraud can also put businesses at risk of noncompliance with industry regulations and standards, such as the Payment Card Industry Data Security Standards (PCI DSS). Failure can result in fines and legal actions.

Operational disruption: Payment fraud can cause operational disruption for businesses if they need to investigate and resolve fraudulent transactions, update security measures, or implement new policies and procedures to prevent future fraud. This can divert resources from other critical business functions and impact productivity and efficiency. Plus, it should be kept in mind that fraud prevents the implementation of one-click payments. Fraud prevention isn't only concerned with mitigating the losses associated with fraud, it also helps preserve the company's ability to focus on more constructive tasks.

Chargeback fees: If a customer disputes a charge on their credit card bill, the business may be required to pay a chargeback fee. Additionally, many payment processing providers charge additional fees to businesses that have a higher chargeback ratio.

Broader economic consequences: Widespread payment fraud can have broader economic consequences, affecting consumer spending, investor confidence, and overall economic stability. Businesses that fall victim to identity theft or credit card fraud may also see negative effects on their credit scores, affecting their ability to secure loans or financial services.

Attacks on the ways businesses handle mobile payments can be swift and cost organizations millions within a short period of time. As an example, a UK bus company, Ensignbus, has banned customers from Monzo and Revolut[19] from using their smartphones to pay for fares and has slashed mobile contactless limits to just £10 following a spike in debit and credit fraud across the network.

Because of the rise in fraud using Apple Pay and Google Pay, the Essex bus company no longer accepts both digital wallets.

The reduced contactless limit affected all users trying to pay via iPhones and Android devices, while transactions from Monzo, Revolut and ABN Amro apps have been blocked at the ticket machines.

[19] *"Fraud Spike Forces Bus Company to Ban Online Banks and Cut Mobile Contactless Limits", Finextra News, 24 August 2022 - https://www.finextra.com/newsarticle/40858/fraud-spike-forces-bus-company-to-ban-online-banks-and-cut-mobile-contactless-limits*

How DCB Fraud Threatens Telcos

Online transactions threats in the DCB subscription model have become problematic especially for telecom operators. India-based software company mFilterit thinks* that the DCB subscription model has made carriers more vulnerable to online transaction threats for a variety of reasons. Here are why these threats are problematic for MNOs:

1. Loss of Consumer Trust and Market Credibility

DCB customers have put their faith in the MNOs. But when it comes to financial fraud, cybercriminals' flagrant disregard for the trust of their victims is still evident. Furthermore, the users accuse MNOs and retailers of embezzling money from them for unfulfilled VAS subscriptions that keep coming up on their invoices. However, cybercriminals' blatant disregard for consumer faith remains obvious during financial fraud.

The telco network suffers a financial setback due to revenue loss from having to reimburse a greater number of users, even while consumer complaints are still on the rise. As such, the brand custodians must fight a never-ending war to ensure the brand's legitimacy and win back the people's trust.

Customers fall prey to financial fraud on other related apps in addition to fraud in the brand's DCB transaction-based apps. Users' digital identities are reportedly sold on the dark web for as little as $25, according to a study.

2. Disables Telco from Achieving the Highest ARPU

According to a report, the prepaid Average Revenue Per User (ARPU)- estimated revenue generated by telcos/MNOs/brands based on active app users in a given period- before the DCB service launch was $9 in Chile, Latin America and post-launch was $19, which included an increase of $10 on core services and $9 on DCB. The same report also states that DCB also enhanced the subscription of core services (20%), prepaid recharge amounts (12%) & recharge frequencies (85%) for Telefonica prepaid subscribers.

Brands may lose out on such possible revenue due to DCB fraud. Furthermore, victims of DCB fraud frequently transfer to other mobile network operators (MNOs) that provide safe subscription payment options and do not tack on extra charges to carrier bills. In addition, clients may come to doubt the value of DCB subscriptions and discontinue DCB services altogether. (ARPU is also a term used in advertising for determining the campaigns generating the highest revenue, deciding the total number of user acquisitions for achieving revenue targets, deciding customer base, pricing strategy, etc.)

3. Drains the Digital Advertising Efforts

Globally, mobile network operators frequently use search engines and other platforms to promote their value-added services. VAS mobile advertising accounted for 54% of Google Ads' ad sales in 2019, with affiliate networks producing the remaining advertising traffic. The next year saw an 8% increase to 62% in the share of Google Ads for VAS mobile advertising.

Whenever customers using DCB as payment for VAS subscriptions become victims of DCB fraud, their trust in the MNOs is lost. Moreover, customers often criticize DCB service providers for the additional charges on their bills for unrendered services.

As a result, clients are less likely to click on MNO ads, particularly on social media, where the share was 17% as of 2020.

* *"Why is DCB Fraud Problematic for Telcos?" mFilterIt blog, June 21, 2022 - https://www.mfilterit.com/blog/why-is-dcb-fraud-problematic-for-telcos/*

03

FRAUD ATTEMPTS & DCB IN THE MIDDLE EAST

Overview of DCB Fraud in the Middle East

In the Middle East, it's much more common for people to rely on mobile payments rather than credit or debit cards. The reason for this is that credit card ownership is not widespread across these countries. The high percentage of mobile phone ownership has given rise to the use of mobile payment methods. Local payment methods such as direct carrier billing and mobile wallets are typical for digital content purchases in the Middle East. Depending on the country, DCB accounts for up to half of digital gaming purchases in the region. However, this diverse and fast-growing market is also targeted by cybercriminals in the Middle East too.

The average fraud attempt rate in the region is 10.3%.[20] (In Europe, it was measured as 5,6%[21].) Two Middle Eastern countries that seem to make perhaps the most notable progress with positive ratings towards security (Kuwait and the United Arab Emirates) have fraud rates of 8.6% and 6.8%, respectively. The following distribution graphics of the pie chart show the types of fraud detected in these two Middle Eastern countries.

As can be seen, the move towards cashless transactions is particularly significant in the United Arab Emirates. The widespread adoption of DCB by mobile operators opens up huge opportunities in this market. However, the UAE's attractiveness as a target for cybercriminals requires robust security measures to protect this payment method.

Kuwait, on the other hand, is experiencing a significant increase in DCB potential, primarily due to increased security measures and a growing demand for contactless payments. Digital payments, including mobile wallets, are becoming increasingly popular as part of the country's digital transformation. This trend positions DCB as a key player in shaping Kuwait's future payments landscape.

[20] "Fraud Report on Carrier Billing 2024 Middle East," p. 2, Evina, 2024 - https://www.evina.com/resources/fraud-report-middle-east/

[21] "Fraud Report on Carrier Billing 2024 Europe," p. 2, Evina, 2024 - https://www.evina.com/resources/master-fraud-report-europe/

So, as the figures below also show, it is important to balance the exploitation of DCB's opportunities with the need for strong cybersecurity measures in both countries.

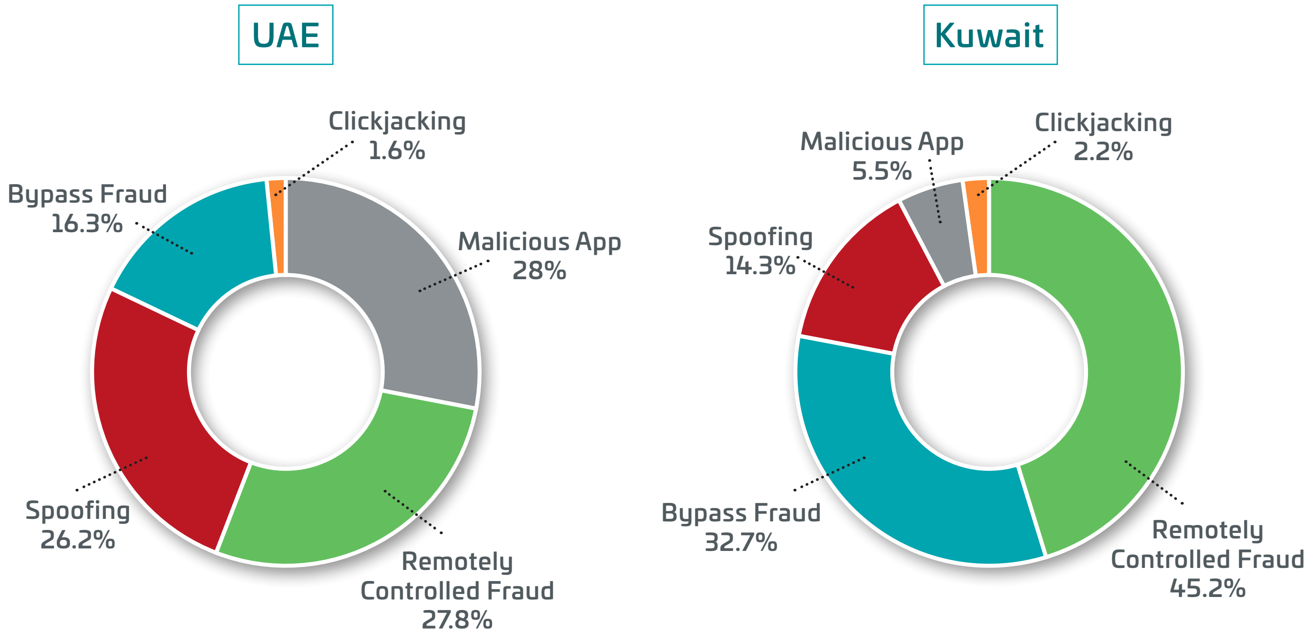
Different DCB Fraud Techniques in the Region

In its research on carrier billing fraud, Evina, one of the most advanced cybersecurity technology companies, enlightens the mobile payment industry about the possible malicious techniques used by cybercriminals, including the latest and most advanced fraud types that were detected on DCB such as:

- ***Remotely controlled fraud:*** Malware takes control of a device to make fraudulent payments. Often, the innocuous user downloads a fraudulent app, such as a gaming app, that gives the cybercriminal access to the user's mobile phone. Then, the cybercriminal takes full possession of the user's phone and, while the user is asleep, launches a browser, subscribes to various services, uses the user's money to do so, and earns a commission on that subscription.
- ***Bypass fraud:*** Short circuits process flow to make payments without clicks. The user browses a website, unaware of its fraudulent nature, and clicks on a fake subscription ad. The fraudulent ad automatically redirects the user to a payment confirmation page without passing by the intermediary steps. The cybercriminal has subscribed the user to a service using the user's money and earns a commission on that subscription.
- ***Spoofing:*** The theft of the network/SIM identity of users to make a payment on their behalf. The user unknowingly downloads a fraudulent app, such as a video game, which turns their phone into a proxy, regardless of whether the app is launched or not. The cybercriminal exploits the user's phone network and SIM identity to subscribe to various services, earning commissions and resulting in the user being billed for these unauthorized subscriptions instead of the criminal.
- ***Malicious apps:*** A mobile application that secretly contains malware, programmed to go through all the flow steps in place of the final user to make payments without asking for the user's consent.
- ***Clickjacking:*** The user is tricked into clicking on a hidden payment button that is disguised as a different button to the eyes of the user.
- ***Code injection:*** Malicious code is injected through a browser flaw to make an unauthorized

Figure 7: Fraud Types in the UAE and Kuwait in 2024

on Carrier Billing



Source: "Fraud Report on Carrier Billing 2024 Middle East," Evina, 2024

automatic payment that is billed to the user.

- *Replay attack:* Transmissions are intercepted and repeated maliciously to make payments.

Statistics indicate that the top three fraud types are remotely controlled fraud, bypass fraud and spoofing. As a very common scam type, remote access fraud is a form of identity theft, in which attacks involve fraudsters deceiving customers into downloading Remote Access Tools (RATs).

DCB Index of The Middle East & Africa

To assess the evolution and potential of DCB for every country, a metrics called "DCB Index"* has been developed by Evina. 2023 edition of the DCB Index for the Middle East and Africa continues to rank countries on a 5-point scale, incorporating new insights into fraud prevention, innovation, local market penetration, and DCB's growth potential. As a result, it offers a detailed analysis of the DCB market's progression and potential in the region, ranking them according to their current DCB status and potential to develop this growth-boosting mobile payment method further.

The DCB Index 2023[22], a collaborative effort between Evina and Telecoming, compares DCB's development in the first half of 2023 to the same period in 2022, while also considering anticipated growth for 2024. The partnership of the two companies leverages their respective expertise in DCB experiences and protection to craft a comprehensive market analysis. Rating the state of DCB and its potentiality, the DCB Index uses a 1 to 5 rating scale, where 1 is the lowest and 5 is the highest level of DCB development and potential.

Notably, the 2023 ranking shows a modest increase in the overall level of security among DCB players operating in the MEA region. The comparison indicates an overall increase in its rating, moving from 2.8 to 2.9. The improvement signals the market's advancements in innovation and opens doors for further development, especially in anti-fraud technology. New countries like Algeria, Botswana and Saudi Arabia have also been included for the first time, providing a more comprehensive overview of the region's DCB landscape.

Roberto Monge, Chief Operations Officer at Telecoming, a company developing monetization technology for sports and entertainment, commented[23] on the progress made by the Middle East & Africa region: "As per the latest DCB Index analysis, mobile penetration in Africa and the Middle East will surpass 90%. This significant growth reflects the expanding accessibility of mobile services across these regions. Notably, our findings show an impressive rise in innovation, with the indicator climbing an average of 3.4 points out of 5 this year alone. This trend is joined by the substantial growth of the most innovative new mobile payment solutions. These advancements are vital in driving the mobile economy, where DCB has already established a prominent presence. Telecoming is witnessing the region's dynamism and the exciting developments currently shaping the market."

* *Let's keep in mind that the DCB Index is intended for information purposes only and is non-binding. The figures provided are algorithm-based estimates calculated from data collected by Evina sensors and Telecoming intelligence*

[22] *"DCB Index 2023," The Middle East and Africa Edition, 2023 - https://www.telecoming.com/wp-content/uploads/2023/12/DCB-INDEX-2023.pdf*

[23] *"DCB Index 2023 Highlights New Market Entrants' Strong Performance" – Telecoming blog, December 13, 2023 - https://www.telecoming.com/blog/2023-dcb-index-by-evina-and-telecoming/*

> Regarding performance comparison among the countries in the region, Morocco emerges as a leader in the DCB Index ranking of 2023 with the highest score (3.6 out of 5), underscoring its robust and reliable Direct Carrier Billing market.

Looking at the figures, David Lotfi, CEO of Evina, highlights[24] the risk of unprotection: “The positive trend is welcome but should not mask the growing disparity in security levels between players. Some players are investing in their development and security on the DCB and reaping significant benefits in terms of growth and profitability, while others are caught in a downward spiral where they find themselves unprotected and under attack by fraudsters who target the least protected regions of the world and avoid defended players.”

When it comes to performance comparison among the countries in the region, Morocco emerges as a leader in the DCB Index ranking of 2023 with the highest score (3.6 out of 5), underscoring its robust and reliable DCB market. Almost all mobile players are deploying DCB, and that’s why Morocco’s DCB market is a reliable and consistent sector. Its runner-up, South Africa (3.5), shows significant adoption of mobile money and potential for DCB growth. The Index also helps to enhance Ivory Coast as the fastest-growing market and draws attention to the increasing market dynamics in Africa. Egypt (3.5) and Iraq (3.5) differentiated by opening more opportunities for DCB deployment and increasing their protection against fraud attempts. Focusing on the Middle East, Kuwait and the United Arab Emirates are making notable progress with positive ratings, as Saudi Arabia comes with an impressive 3.4 rating, demonstrating its relevance and boosting the region’s average score.

Now, let’s see how 2023 edition of the Index used its algorithm to evaluate and craft a comprehensive analysis of DCB's potential in each country and a rating score. (If you wish to see the ratings of the DCB development and potential of all countries covered by the DCB Index 2023, please refer to the full report.)

DCB Progress and Performance in MENA

ALGERIA (2.9): Algeria's DCB market, with its strong potential for development, presents a distinct DCB landscape. While all local mobile network operators provide direct carrier billing, the market is challenging to penetrate externally due to stringent regulations and specific operational methods.

BAHRAIN (2.9): Bahrain is only slightly ahead of in 2022, mainly because DCB penetration among mobile operators has reached 100%. However, the sector is increasingly vulnerable to sophisticated and targeted cybercrime. This vulnerability can be mitigated by appropriate DCB protection measures.

EGYPT (3.5): While still in its early stages of expected significant growth, Egypt’s DCB market is showing signs of improvement in cybersecurity. Despite being a target for cybercriminals, many players have begun enhancing their protections. Coupled with the country's high innovation potential and the increasing popularity of digital payments, DCB is poised for sustainable growth in a market where cash has traditionally dominated.

IRAQ (3.5): Iraq is experiencing a maturing DCB market characterized by improved security and increased innovation, exemplified by forward-thinking partnerships in the fintech sphere, such as ZainCash with Western Union. While there's room for further development, the market is becoming more secure and sustainable, with anticipated cybersecurity collaborations in 2024.

IVORY COAST (3.1): Ivory Coast has shown increased DCB potential since 2022, marked by a heightened push for innovation in the fintech sphere, evident in developments like the personal finance app Djamo. In addition, DCB players have

[24] *“DCB Gains a Strong Foothold, Boosting the MEA Region DCB Index rating,” Evina Press Release, 13 December 2023 - https://www.evina.com/press-releases/direct-carrier-billing-gains-a-strong-foothold-boosting-the-mea-region-dcb-index-rating/*

> South Africa is a frontrunner in the African DCB market, with significant growth potential. Mobile users are quick to adopt alternative payment methods such as mobile money, which reached 8 million users in South Africa in 2023.

shifted towards improving the customer experience through enhanced security for DCB users. These developments have laid a solid foundation for DCB, allowing players to continue to focus on innovation and diverse DCB services.

KENYA (2.9): In 2023, Kenya's carrier billing market has achieved a level of stability and continues to exhibit considerable potential. Despite the persistent threat from cybercriminals targeting DCB, the market is poised for stronger defences. With more cybersecurity collaborations anticipated in 2024, the Kenyan DCB market will strengthen its resilience.

KUWAIT (3.0): Kuwait's DCB potential has seen a notable rise, particularly due to enhanced protective measures. The increasing demand for contactless transactions is the catalyst in this trend. As digital payments, including mobile wallets, continue to drive the country's digital transformation, DCB is poised to play a crucial role in shaping Kuwait's future payment landscape.

MOROCCO (3.6): Characterized by stability and robust protection against technical fraud, Morocco’s DCB market is a reliable and consistent sector. This stability has allowed for steady, albeit gradual, revenue growth without the disruptions of 'stop and go'. The market's resilience and steady progress point to a solid foundation for future DCB development.

QATAR (2.9): In Qatar's appealing and innovative direct carrier billing market, the risk of fraud by cybercriminals poses a challenge to securing growth. Addressing this through enhanced security measures can unlock further potential. A stronger commitment from DCB players to effective fraud protection is critical to strengthening the security and resilience of the DCB ecosystem in Qatar.

SAUDI ARABIA (3.4): Saudi Arabia offers a significant DCB market, yet it poses unique challenges. Strict compliance regulations can incur substantial costs for DCB players if not adhered to rigorously. However, this is offset by the country's commitment to security, notable innovation, and widespread DCB adoption.

SOUTH AFRICA (3.5): South Africa is a frontrunner in the African DCB market, with significant growth potential. Mobile users are quick to adopt alternative payment methods such as mobile money, which reached 8 million users in South Africa in 2023. This trend, when combined with effective cybersecurity, will enable DCB to boost revenues for mobile players significantly.

TUNISIA (2.9): The momentum of innovation, driven by major players such as the Tunisian Post Office investing heavily in digital payment services, is pushing DCB in a promising direction. Mobile players should prioritize innovation and cybersecurity to create DCB as a widely accepted payment mechanism and revenue stream.

UNITED ARAB EMIRATES (3.3): With 1.7 million underbanked people in UAE and the market moving towards cashless transactions, DCB has a huge window of opportunity. All mobile operators continue to offer carrier billing to pay for services. However, it’s imperative to safeguard this payment method as the UAE is a prime target for cybercriminals.

Saboteurs of Africa’s DCB Potential

Thanks to its convenient character and the 10x better conversion rate, DCB is, without a doubt, a major revenue opportunity for MNOs. Many known mobile carriers today use this payment method. The fact that there are five times more mobile phones than credit cards in the world today helps its continuing progress as a payment method.

“The main obstacle that makes it difficult for carrier billing to reach its full potential is fraudsters,” says[25] Luis Vicedo, CTO at Digital Virgo, mobile

[25] *“Combating Fraud in Carrier Billing,” DV Pass, November 12, 2020 - https://www.digitalvirgo.com/combating-fraud-in-carrier-billing/*

payment expert: "… as this payment method only works if flows are secured and if the payments of end-users are protected. Once fraudsters are dealt with, by applying the right anti-fraud solution, fraud risks become very limited and carrier billing establishes itself as one of the most competitive payment methods on the market. Today, carrier billing serves mostly digital goods; soon we expect DCB to cover physical goods, services and even loans."

Some security vulnerabilities are not the only problematic aspect of DCB. There are some more hurdles across the growth path. Although we see modest progress in the overall performance of DCB in MENA countries, mobile payment players are struggling to achieve the same success on Direct Carrier Billing (DCB) as they did on mobile money, which was up to 23% in 2023. The struggle is especially prevalent in Africa. Investigating the reasons beyond this fact, Christian Calcagni, Market Director at Evina, had in-depth and enlightening discussions with top DCB professionals in Africa. Calcagni then narrowed the problem down to just three saboteurs. In his recent article titled "The Three Saboteurs of Africa's DCB Potential"[26], Calcagni highlighted the challenges of Direct Carrier Billing (DCB) in Africa. He thinks that key players are deterred from investing in DCB, even in their established markets. A surge in fraud due to ineffective solutions and wrongful blocking of legitimate transactions (false positives).

As a result, regulators unable to relax the DCB's operational framework, do not give the green light to experimental pilot projects, such as click-flows. According to Calcagni, here are the 3 main saboteurs of DCB potential, affecting its adoption and deterring key players from investing in this promising payment method:

Unreliable Partner: DCB's success hinges on solid coordination and trust among operators, payment aggregators, and merchants.

- When an operator neglects payment timelines, it jeopardises its aggregators and merchants. Many are reluctant to enter certain markets because of poor payment terms and uncertainty about receiving payments on time.
- When a merchant does not monitor its flows against fraud, it threatens the credibility of its partner aggregator and risks being excluded from the DCB business.
- When payment aggregators fail to meet compliance standards, they jeopardise the viability of the entire DCB ecosystem, particularly when complaints come from VIPs or numerous victims.

Bad Fraud Fighter: While most DCB stakeholders fight fraud, not all approaches are effective.

- In operational terms, this can mean arbitrarily limiting the number of partners joining an operator's network, complicating payment flows by introducing user-unfriendly steps and a constant stop-and-go approach (stopping DCB and then restarting it) that exhausts partners.
- Technologically, relying on outdated, off-the-shelf solutions that lead to numerous false positives and fail to detect actual threats, such as hacking and user manipulation.

The Regulator Avoider: Then there are those who neglect regular engagement with regulators, viewing regulation solely as a mere business constraint. This approach is disastrous:

- Regulators remain uninformed about the health, dynamism and quality of the sector, preventing the introduction of incentives such as regulatory sandboxes and increased payment thresholds and scopes.
- Relationships with regulators are only built when things go south, affecting the market as well.

[26] The Three Saboteurs of Africa's DCB Potential," Christian Calcagni, January 31, 2024 - https://www.linkedin.com/pulse/three-saboteurs-africas-direct-carrier-billing-christian-calcagni-mrgmc/

04

HOW TO PREVENT MOBILE PAYMENT FRAUD

Best Anti-Fraud Practices

It is needless to say that fraud is a problem that affects all players in the mobile payment ecosystem: the consumer loses money, carriers lose revenue and incur extra customer service complaints, and merchants lose brand reputation. Powerful and complete anti-fraud tools and techniques are therefore essential to be able to make mobile payments such as Direct Carrier Billing (DCB) a foolproof payment process. DCB will become an effective tool for all market players, especially Mobile Network Operators (MNOs) to effectuate daily secure transactions in this era of digital monetization.

The Mobile Ecosystem Forum (MEF) kicked off a new workgroup some time ago to tackle fraud related to DCB. The cross-stakeholder group is currently developing a fraud framework to seek industry alignment and help market education to ensure a sustainable trusted channel. MEF and its DCB Fraud Group are working hard to combat fraudster attacks targeting the DCB channel. One important component is best practices. The group's aim is to share knowledge and best practices so that there is greater awareness and DCB fraud can be minimised. Here are four simple best practices recommended by the group[27]:

Know your 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.

Know your traffic: Your market activities 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; do device-level monitoring and analysis.

Know your partners: Some basic considerations to make when selecting an anti-fraud partner include: conducting a reputational analysis and scrutinising their historic records; confirming they know what's running on the network; making sure they have access to transactions and download data; using fraud detection that covers both IP addresses and the device; and ensuring any party that has committed fraud cannot re-enter the product channel.

MEF's DCB Fraud Group also comprises anti-fraud specialists whose technical solutions can detect and eliminate anomalies to identify questionable traffic and transactions. These systems combine machine learning algorithms with payment processing workflows to block fraud in real-time. Providers include Evina, Empello, MCP Insight, mFilterIt, and Upstream.

Their products work by placing a sensor on a payment page, which scans activity patterns and compares them to fraud patterns. When there is a match, it prevents the fraudulent transactions from going through. It then displays the traffic analysis results on a dashboard.

[27] *"MEF Anti-Fraud Yearbook 2023," Mobile Ecosystem Forum, p. 35, 2023 - https://mobileecosystemforum.com/mef-anti-fraud-yearbook-2023/*

> The MRC report aims to deliver clear and impartial insights into the perceptions and evolving trends in e-commerce payments and fraud as observed by merchants worldwide.

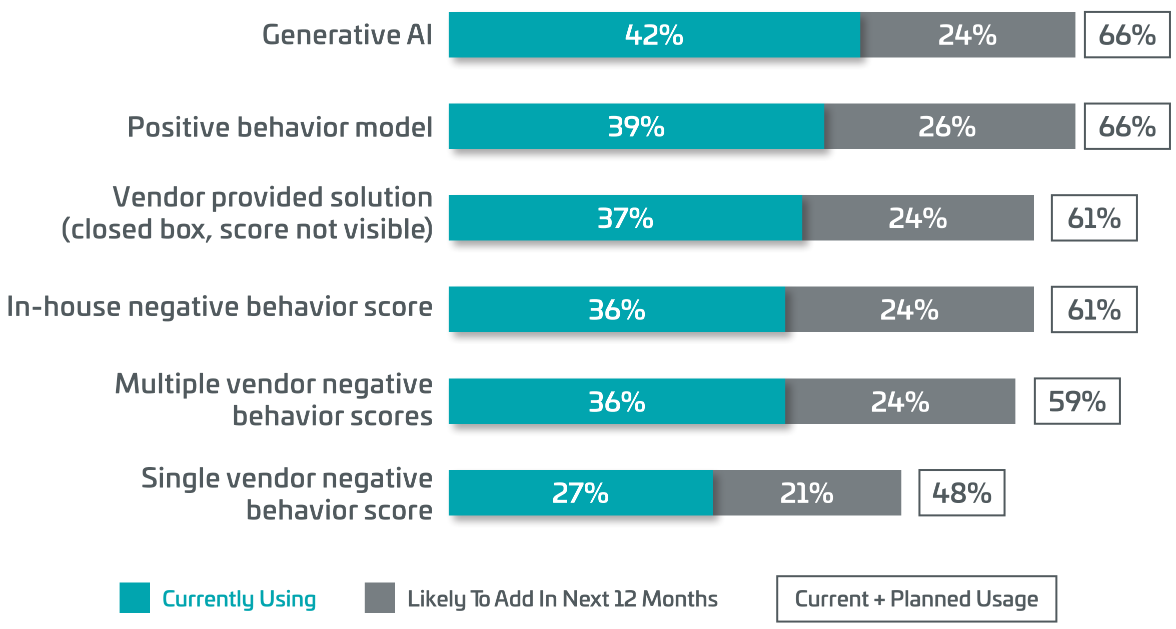
Fraud Management Toolkits

When it comes to specific tools and techniques merchants employ to monitor and prevent fraud across the customer journey, "2024 Global eCommerce Payments and Fraud Survey" has a lot to put forward. The Survey was conducted by The Merchant Risk Council (MRC), a global non-profit membership association connecting e-commerce professionals through industry-leading educational programs, online community groups, conferences, and networking events. Advocating for safer and more profitable e-commerce for everyone, MRC, in collaboration with Visa Acceptance Solutions and Verifi unveiled the findings of the Survey. Drawing observations from a wide spectrum of businesses across more than 35 countries, their report[28] aims to deliver clear and impartial insights into the perceptions and evolving trends in e-commerce payments and fraud as observed by merchants worldwide. As an authoritative guide to empower merchants with knowledge for strategic decision-making in payment management and partnerships, the report also focuses on fraud-fighting tools driven by AI and/or ML.

According to "The 2024 Global E-Commerce Payments & Fraud Report," merchants are using globally an average of one to two different AI/ML-driven fraud management tools; however, as shown in the relevant figure below, none of the six tools tested in the survey is currently in use by more than 50% of merchants. But adoption of these tools is likely to grow swiftly. No doubt, these advanced solutions will quickly become central tools in merchants' anti-fraud toolkits as they are implemented and integrated into their IT systems over the coming months.

Figure 8: Fraud Management Tools & Techniques

Merchants' Current & Planned Usage of AI/ML Driven Tools



Source: "The 2024 Global E-Commerce Payments & Fraud Report," MRC, p.59, 2023

[28] *"The 2024 Global E-Commerce Payments & Fraud Report," The Merchant Risk Council (MRC) in Partnership with Visa Acceptance Solutions and Verifi, p. 59, 2023 - https://merchantriskcouncil.org/learning/mrc-exclusive-reports/global-payments-and-fraud-report*

USE CASE

How a Turkish Payment Provider Increased Customer Satisfaction While Decreasing Fraud with a Cybersecurity Solution for DCB

• CHALLENGE

Founded in 2015, Payguru (TPAY Türkiye) was the first mobile payment company to be granted a payment license from the Turkish financial regulator. TPAY, the full-service digital payments aggregator for the Middle East, Africa, and Türkiye, acquired Payguru in December 2020. Türkiye was such a market that the market regulator (the Turkish Central Bank) implemented harsh restrictions and even closed the alternative payments market entirely in 2018, due to fraudulent transactions. TPAY Türkiye undertook a challenge to help create a healthier mobile commerce ecosystem in Türkiye with clean traffic, free of fraudulent transactions, where users do suffer because of fraud and therefore the regulatory body would not see the need to implement restrictions or close the market.

This task was also important for the merchants, whose efforts to achieve sustainable growth would not be hindered by fraudulent traffic at the hands of cybercriminals.

TPAY Group CEO Işık Uman said: “Whenever consumers become victims of DCB fraud, their trust is lost not just in the aggregators or carriers but also in the merchants. So, we wanted to prove that DCB is as safe as any other payment method as long as state-of-the-art fraud prevention solutions are implemented.”

The successful implementation of AI-driven DCBprotect, Evina’s most advanced cybersecurity solution, helped block direct carrier billing (DCB) fraud attempts in real-time and yielded flawless DCB payment flows.

• SOLUTION

Partnering in February 2022 with Evina, a leading cybersecurity solution provider, TPAY Türkiye entrusted their cybersecurity solution for direct carrier billing (DCB). Turkish team integrated Evina DCBprotect into their platform as an extra security layer and began monitoring the transactions traffic. Kemal Savcı, Business Operations & Product Management Team Leader at Payguru, explains: “Consumers are being exposed to DCB fraud risk mainly from two different sides. The biggest threat comes from the attackers targeting the advertising space – using technical methods to win pay-outs for bogus clicks. In some cases, it leads to unwanted subscriptions. Another threat is “social engineering,” in which fraudsters pretending to be someone else initiate a transaction, contact an account owner and ask for the PIN code. If the consumer shares it, they get charged.” With the monitoring tools of DCBprotect, Savcı witnessed that 90% of fraudulent attempts on TPAY Türkiye’s transactions are remotely controlled fraud, meaning the cybercriminals attempt to make fraudulent payments through malware that takes control of a device.

Once the 4-month pilot process was a success, official activation was put into effect in late July 2022 to detect and help block fraud attempts on carrier billing transactions in real time. From the begining of the implementation, it was observed that DCBprotect detected 99.94% of fraudulent transactions with a 0.06% false-positive rate and <100ms latency.[29]

• RESULTS

The successful implementation of AI-driven DCBprotect, Evina’s most advanced cybersecurity solution, helped block DCB fraud attempts in real-time and yielded flawless DCB payment flows. The major fraud rate drop from 60% to 20% in a couple of days was due to the blocking of fraudulent traffic. The cybercriminals completely stopped sending traffic as it was no longer converting. The fraud spike on August 7th was due to a new fraud pattern detected by Evina (on August 8th) and blocked right away. As soon as the new fraud pattern was identified, the fraud rate plunged back down again without affecting the number of authentic transactions.

[29] *“Consumer Complaints Decrease, Trust Strengthens,” Payguru Case Study, Evina, 2023 - https://www.evina.com/resources/payguru-x-evina/*

As expected, billed transactions slightly decreased in the beginning after the full implementation of the DCBprotect solution. However, the billed transactions started to increase again on an upward trend.

As a result, the decrease in fraudulent transactions clearly did not affect the Turkish operator's (Turkcell) billed transactions; it simply required the expected adjustment time. In less than 3 weeks of time, Turkcell's billed transactions got back to pre-DCBprotect volumes. Afterwards, authentic and billed transactions increased simultaneously. Thanks to DCBprotect, fraudulent traffic was not allowed anymore and was blocked immediately. TPAY Türkiye merchants stopped spending on fraudulent traffic, resulting in a bigger budget to buy traffic from cleaner sources, which enabled the addition of new traffic sources and thus increased traffic volume.

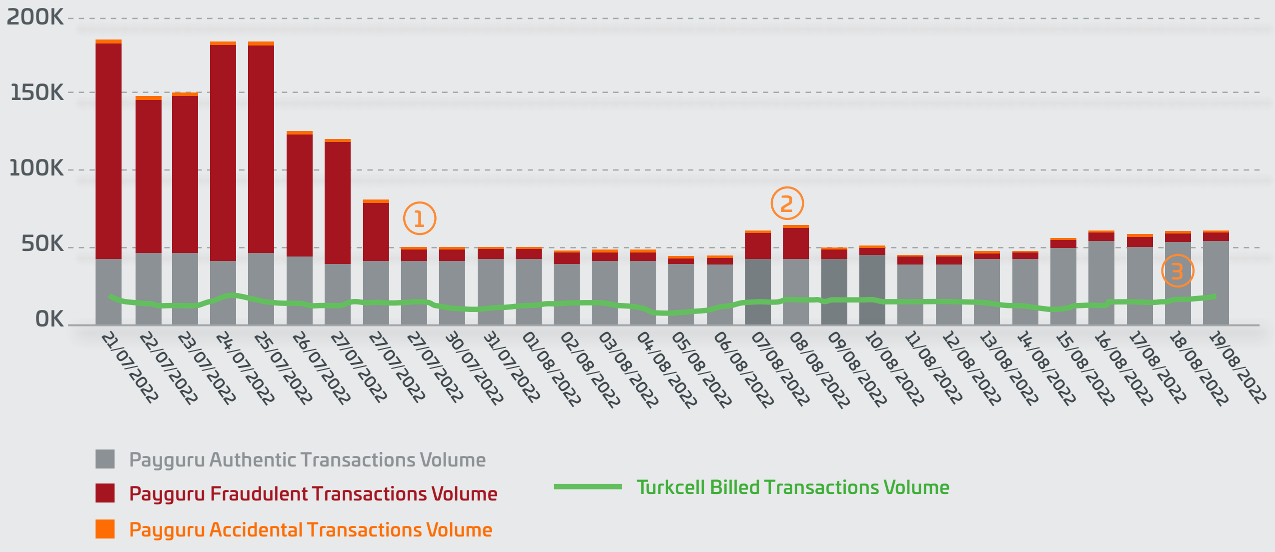
In the long term, revenues become healthier as they are not muddied by fraudulent transactions, and the brand image improves. In addition, the cost of handling complaints decreases, and customer satisfaction increases, which allows for healthy and sustainable revenue growth. David Lotfi, CEO of Evina said: "In an ecosystem as complex as the mobile payments market, Payguru needed to implement advanced cyber protection, as it sometimes only takes one weak link for cybercriminals to bypass protections and steal money. Thanks to our proprietary technology developed over 15 years, we are now able to identify and block fraudulent transactions better and faster than anyone else."

• MAJOR BENEFITS[30]

- A dramatic decrease in suspicious transactions (-80%)
- User complaint rate decreased rapidly (-50%)
- A sharp drop in refund amounts for charges billed without consumers' consent (- 45%)
- Renewed consumer trust in the DCB ecosystem due to proof of traffic authenticity
- Easier expansion into new markets with improved brand reputation
- Significant budget savings thanks to the elimination of paid traffic sources of unclean nature

Figure 9: Evolution of the Traffic and Transaction

Volume Change Since Implementing Evina DCBprotect.



Source: Payguru Case Study, Evina, 2023

[30] *"How Payguru Increased Customer Satisfaction," Payguru - Evina Case Study, Payguru July 26, 2023 - https://tpaymobile.com/through-the-implementation-of-cutting-edge-anti-fraud-solutions-tpay-turkey-payguru-achieved-a-remarkable-elevation-in-customer-satisfaction/*

Tips to Minimize the Risk of DCB Fraud

Digital Virgo - an expert in the field of Telecom Payment - in collaboration with its partner Evina -an expert in mobile fraud - worked together in order to put forward with the ten essential tips[31] to minimize the risk of fraud in the DCB ecosystem. The ten tips are as follows:

1. Be aware of having a full understanding of the DCB ecosystem
2. Audit your risk & assess your level of exposure
3. Get organized, fraud is a subject that needs to be dealt with
4. Implement continuous real-time monitoring in order to identify unusual patterns
5. Compare and analyse user behaviour to detect suspicious users
6. Get total control of end-user flow by hosting the customer's confirmation page
7. Integrate Business Intelligence tools to identify possible sources of fraud from the business KPIs
8. Rely on experts to analyse your Data
9. Make sure your traffic sources are trusted
10. Set up a validation process for the incoming traffic

Conclusion

In terms of payments, merchants are aware that as more customers use new mobile payment methods, fraudsters will find it more and more appealing to target these methods. Despite this, merchants are continuing to extend their acceptance offerings.

The proliferation of mobile payment methods such as DCB and mobile wallets, payment fraud types, and payment management tools and approaches has placed businesses under increasing pressure to monitor and evaluate a wide range of payment-related metrics. For many, maintaining a consistent and logical approach to payment monitoring and assessment may prove to be an increasing issue in the future.

According to reports, one of which was conducted by the Merchants Risk Council as the 25th edition of Global E-Commerce Payments & Fraud (2024), retailers are dealing with a persistent rise in several types of fraud, with first-party abuse rates rising especially quickly.

Merchants are attempting to control first-party misuse and other common fraud issues by implementing comprehensive strategies that make use of a variety of tactics and solutions. These include strategies and technologies related to identity and verification, improved requirements, and flagging and checking. They also involve using the updated compelling evidence guidelines of card brands to prevent or reverse first-party misuse disputes.

There is never a "one size fits all" solution in the industry since different merchants have different objectives and methods for managing and preventing fraud. Some prioritize the customer experience as their top priority, while others

[31] *"10 Tips to Avoid Fraud in DCB Ecosystem," Digital Virgo, 23 July 2020 - https://www.digitalvirgo.com/tips-to-avoid-fraud-in-dcb/*

> Financial scams are like the multiple-headed hydra from Greek mythology, where every time one scam is exposed, many more emerge in its wake. Recent history has seen the evolution of cons, notable impersonation and romance scams, which have a significant financial and emotional toll on victims.

concentrate more on chargebacks and fraud reduction. We all hope that in the future, there will be more research into the most effective tactical and strategic tactics as merchants, payment aggregators, and operators, together with the regulators, increase to collaborate against fraud in the intricate landscape of today's mobile commerce. Because the fight against these criminal gangs is a collective responsibility that extends to all regulated firms. In today's digital age, this is possible in practice if all the parties involved in the payment ecosystem collaborate by providing verified payment options.

The words of Myron Jobson[32], senior personal finance analyst at Interactive Investor, summarize the necessity of a collective anti-fraud fight beautifully:

"Financial scams are like the multiple-headed hydra from Greek mythology, where every time one scam is exposed, many more emerge in its wake. Recent history has seen the evolution of cons, notable impersonation and romance scams, which have a significant financial and emotional toll on victims. The internet continues to be a rich trolling ground for unscrupulous individuals to convince unsuspecting victims to part with their hard-earned money. Fraudsters are only too willing to exploit any ignorance or naivety."

When it comes to fighting fraud in mobile payment, including organized crime activities, compliance, and the prevention of illicit funds movement in the financial system, in recent years, there has been a significant increase in the adoption of new technologies and efforts by major financial institutions.

Machine learning (ML), Artificial Intelligence (AI) and data analytics have all emerged as powerful technologies among the innovative regulatory technology application use cases, including risk assessment, regulatory change monitoring, compliance reporting, communications security and compliance, Anti-Money Laundering (AML) policies and laws, and Know Your Customer.

Merchants and payment solution providers must deploy fraud prevention technologies and tools to tackle various types of fraud efficiently, remain compliant with international regulations, and create a frictionless user experience. Financial institutions, too, must invest in the necessary resources and expertise to implement these technologies effectively. However, it should not be forgotten that these technologies are only as good as the data, and if that data is biased or incomplete, it can lead to inaccurate or unfair results.

The main topics covered in this whitepaper prove their relevance not only in understanding the complexity and the scale of global fraud and its financial damages but also in creating new, successful anti-fraud strategies that consumers, merchants, and payment solution providers can implement to deter. We hope this whitepaper has provided relevant tips and strategies to help ecosystem actors step into the future more ready than ever to combat the negative economic impact of fraud and to deliver a frictionless, fraud-free experience for the end-user.

[32] *"Industry Calls for Enhanced Collaboration to Tackle Ever-Expanding UK Fraud Levels," The Fintech Times, October 26, 2023 - https://thefintechtimes.com/industry-calls-for-collaboration-to-tackle-uk-fraud/*

CONTACT

TPAY MOBILE HEAD OFFICE
1509 Fifteen Floor,
Thuraya 1, Tecom, Dubai,
United Arab Emirates
Tel: +971 436 16 339
www.tpaymobile.com

CAIRO OFFICE
30A, Ibn Malka St.
First Settlement Service Zone
First Settlement, New Cairo
Cairo /Egypt
Tel: +20 (0)2 22460081

ISTANBUL OFFICE
Reşitpaşa Mahallesi
Katar Caddesi, Teknokent
ARI 1 Binası, No:2/5/23
34398 Sarıyer
Istanbul/ Türkiye
Tel: +90 (0)212 2854600

LAGOS OFFICE
7b Olu Holloway Road
İkoyi, Lagos /Nigeria
Tel: +234 1280 2330
+234 809 419 0896

RIYADH OFFICE
Office #111, 7961 Takhassusi Road
3367
Al-Mohammadeya,
Riyadh,
Postal Code 12363
KSA
Tel: +966 507163325

For more information, please visit the
TPAY website at **www.tpaymobile.com**