

Tsinghua University Certificate Program on "Innovation & Entrepreneurship for Digital Economy"






E-Commerce Project Group Draft

Project Group Focus:

“Impact of E-Commerce on the development of Africa”

Southern Africa Group

Autumn 2022

NAME	SCHOOL	MAJOR	PICTURE
Ainebyona Moses	Xiangtan University	Masters Degree in, Sinicization of Marxism	
Alec Mabhiza Chirawu	University of Science and Technology Beijing	Master's Degree in, Information and Communication Engineering	
Japhet Patrick Konzo	Southern China University of Science and Technology	Master's Degree in, Computer Science	
	Zhongshan University, Lingnan College	MBA	

Overview of e-commerce in the region

As technology grows to be a bigger part of today's society Electronic commerce which refers to the activity of buying and selling of products or services using the internet and therefore the transfer of cash and data to execute these transactions has become an essential way for business to trade with online shopping leading the way Although electronic shopping is progressively becoming popular globally nevertheless in South Africa it continues to experience slower growth rates. The purpose of study is to explore describe analyze and get a better understanding of the South African electronic retailing operations and the role it plays in the country's economy as a whole by reviewing the South African shopping categories, popular e-commerce firms e-commerce models and the current market trends The paper focuses on investigating the factors affecting the growth of ecommerce in South Africa, to investigate the barriers to entry for small medium enterprises in electronic retail and analyzes the perceived benefits of e-commerce. The research methodology approach chosen for this study was the mixed research approach. Data was gathered or collected from a total number of 255 participants from Cape Town South Africa using a close-ended questionnaire and interviews. The results of the study show that most South Africans have access to the internet via cell phones also the study outcome showed that the South African e-commerce rank is globally lagging behind because of certain barriers to entry by Small Medium Enterprises. The results were conclusive on infrastructural barriers which include; internet security, internet connectivity high installation costs compatibility and lack of education as well as socio-economic barriers and socio-cultural barriers. The study also concluded that the slow adoption of ecommerce has largely been attributed to customer illiteracy, cost of delivery mechanisms the low use of e-commerce amongst customers, low use of e-commerce amongst suppliers high cost of computer hardware and network technologies, and non-dependability of telecommunication services. The study proposed that the South African government should address e-commerce challenges by accessing modern and efficient machines system and provide experienced well-trained technician to assist the customers. The study also proposes that organizations with online presence must identify the risks and threats to security in order to promote a safer security environment for potential electronic customers.

Key Words: E-commerce, South Africa, Online Shopping Retailers SMEs Internet

Trends and the big players in the market & the growth of Mobile e-commerce

New data shows that the South African online e-commerce market has grown rapidly and is currently estimated at just under R200 billion per annum. Companies such as Takealot, Woolworths and Checkers are all adapting to new consumer habits. An increase in the e-commerce estimated value indicates how Covid-19 exponentially accelerated the use of e-commerce.

Before the pandemic, e-commerce accounted for 8% of total card payments spent in the retail space, with 35% of the sector being made up by spending on travel and accommodation. At the end of 2021, e-commerce accounted for 14% of total card payments sales, with travel and accommodation only taking up 11%. “E-commerce has already exceeded our conservative estimates initially published at the peak of the pandemic.

South Africa’s e-commerce market will reach more than R400 billion by 2025 on the back of more than 1 billion transactions per annum, estimated. Statistics show that total online sales in 2020 jumped by 55% and another 42% in 2021, driven by increased spending in less traditional e-commerce industries. Online spending on products – other than travel or accommodation – doubled in 2020 by reflecting a 102% increase which saw an additional 39% of growth in 2021. Transaction volumes remained robust with an estimated 500 million in 2021, up from 200 million in 2019 and 345 million in 2020.

However, people were spending less online with smaller retail and lower basket items gaining traction – the average purchase value of R390 was R60 less than the average in 2019. “Not all major retailers were prepared for the sudden change, but those that were successful were the ones who would adopt a fast, reliable logistical solution in meeting the delivery demand.

Opportunities and challenges

E-Commerce is growing at unprecedented rates in South Africa. Some of this growth has undoubtedly been fueled by the coronavirus pandemic, and while it remains to be seen if the demand will hold up, the expectation is that culture is shifting for the long term. The increased appetite of South Africans for online shopping has not gone unnoticed by retailers as they seek to offer customers greater freedom and more options to transact. More and more businesses, both small businesses and established retail giants are following the demand and are establishing e-commerce as an essential sales channel. Also, the rise and rise of mobile and internet penetration is laying the foundation of more day-to-day activities, including shopping, going digital.

For this digital revolution to be completed, however, the players in the market need to innovate and invest in overcoming the challenges that belabor the e-commerce sector in South Africa. Data costs remain incredibly high, the residential addressing system is not well defined, and access infrastructure such as the internal road and rail system is not up to par. Insecurity also remains high, and many South Africans still have trust issues with shopping and paying remotely. Once these challenges are met, e-commerce in South Africa should be able to break the ceiling and achieve the immense opportunity it holds.

Key challenges to overcome were consumer trust in the fulfillment of sales where physical products had to be delivered, and logistical solutions to meet spiking demand,”

More market competition

The shift to e-commerce has increased the competitiveness of smaller, independent retailers, who recognise that their client base can be expanded beyond their immediate regional presence. Despite larger retailers having bargaining power with potentially significantly lower input costs than an SME going virtual, their digital prices are substantially higher since they need to maintain a unique digital offering whilst ensuring data security. The lure of marketplaces offered by Takealot, Bidorbuy, Facebook Marketplace, and similar solutions have opened avenues for those unable to invest in a professional digital platform to sell their products. Below are some examples of e-commerce growth among some of the country's largest retailers:

Takealot

In April 2021, the Naspers group acquired the share capital held by non-controlling shareholders of Takealot for roughly R830 million. As a result, the group holds 100% effective interest in Takealot. Takealot continued to benefit from the shift to online, growing gross merchandise value by 72% and revenue by 63% for the six months ended September 2021. “The fastest-growing categories were consumables, home, lifestyle and media,” said Naspers. The interim financial results for 2021 indicated that third-party marketplace sales on Takealot outpaced first-party offerings, with first-party retail sales growing 15% and third-party marketplace sales by 55%. Other increases in smaller Naspers e-commerce companies were seen:

- Mr D – As Takealot group’s food-delivery business, Mr D also benefited from the shift in consumer spending to online delivery and saw an increase of 88% in orders.
- Superbalist – The online fashion website saw gross merchandise value increase by 77% despite increasing competition from brick-and-mortar fashion retailers.

Woolworths

According to the unaudited interim group results for Woolworths Holdings Limited, trading conditions earlier in the reporting period [26 weeks ended 26 December 2021] were impacted by the ongoing effects of Covid-19, the civil unrest in July, power outages and international supply chain disruptions, and supplier delays. Despite this, the South African division of Woolworths saw the following increases in online sales:

- Woolworths Fashion, Beauty and Home – Online sales growth of 19.2%, compared to December 2020, contributing to a total of 4.4% of sales.
- Woolworths Food – Relative to the comparative period, overall sales grew by 15.2%, and online sales saw a significant increase of 55.8%, contributing to 3.1% of its food sales.

Woolworths South Africa stressed that their overall expenses grew by 6.3% due to ongoing investment in online capabilities and higher energy costs. As a global group, Woolworths Holdings Limited saw a 22.4% increase in online sales, thus contributing 13.7% to the Group’s total turnover.

Checkers

Shoprite Holdings as the holding company of Checkers released its unaudited results for the 26 weeks ended 2 January 2022. It showed that Checkers was a key driver for the R2 billion increase in the group’s gross profit.

Regarding online engagement and sales, Checkers Sixty60, the group's on-demand grocery delivery app maintained its growth, expanding its services to 266 stores [233 stores in FY 2021], said Shoprite.

Pick n Pay

Pick n Pay's unaudited condensed interim financial statements for the 26 weeks ended 29 August 2021 showed an increase in engagement with the company's online shopping options. "Online clothing sales increased 150% year-on-year (for the first comparable month), with the value of online baskets more than doubling those of in-store purchases," said Pick n Pay.

Online identity verification

Mobile penetration in Africa is growing impressively at about 46% as more people come online for the very first time. In turn, this has increased the market opportunity for startups, especially fintechs and e-commerce, which try to provide various solutions to meet the financial needs of the populace. But to do that, these businesses must carry out certain identity verifications and KYC to combat fraud, among other things. Many platforms power these KYC processes, and one of them, Identitypass, is today announcing that it has raised \$2.8 million in seed funding, months after graduating from Y Combinator. The round also comes a few months after the startup raised \$360,000 in pre-seed investment last November, bringing its total funding to \$3.1 million.

Reports say African businesses lose \$4 billion annually to cybercrime. The global figure for this occurrence stands at \$1 trillion. Thus, the need for fintechs and digital businesses in Africa to perform stringent KYC and verification checks on their customers.

However, for the folks at Lagos-based Identitypass, it wasn't the love for reducing the high rates of fraud that led them to start the company. According to co-founder and CEO Lanre Ogungbe, the team was initially building a platform that required consumers to use biometrics (face, fingerprints or voice) and cards to make payments. But while developing the platform, they encountered issues performing verification checks. Hence, the decision to pivot.

Today, we have basic authentication using OTPs or a four-pin password, but by starting **Identitypass**, more authentication options into the market need to be introduced."

Identitypass approached various agencies and authorities countrywide to get licenses and certifications needed for authorizing checks across a full spectrum of verification points. It launched with one data point in January 2020. But now, 200 active businesses across fintech, e-

commerce, education and mobility connect to 18 data points to verify their customers' identities on the platform.

Ecommerce platforms in Africa

The increasing access to the internet is seeing a rapid emergence of e-commerce sites eager to tap into the continent's growing online consumerism. The likes of Nigeria, Kenya, and South Africa are at the forefront of this evolution. Companies such as Jumia, a Lagos-based online retailer, are dipping their finger in almost all major markets on the continent, cutting themselves an enviable piece of every pie. Jumia is also among Africa's best-funded e-commerce sites, having raised US \$150 million in funding in 2014. As more people take to the internet to do their shopping, the demand for devices such as smartphones also increases.

Some of the top e-commerce platforms in Africa that are reaping the benefits of the booming internet penetration on the continent:

JUMIA

With a mission statement and ethos for connecting African consumers and entrepreneurs to do better business together, Jumia is blazing the trail of e-commerce sites in Africa. The company is creating a platform where small, medium and large African companies link with their potential market, thus creating a new-age ecosystem that bypasses the middle man.

Launched in 2012 in Nigeria, the site has solidified a footprint in over 23 African countries, with a network of over half a million sellers since its inception. Jumia has managed to create a stellar reputation for being a hub for products and services spanning across the retail, food and hospitality, talent recruitment, concierge and the hotel and catering industries. Apart from servicing the needs of consumers and businesses, Jumia has also been upskilling and aiding

employment for many Africans who are qualified in areas such as Engineering, IT and online marketing and web development.

TAKEALOT

South Africa's Takealot is the go-to online retailer for the shopper that seeks a convenient and simplified online buying and user experience. The site has been around for over a decade, having been established in the year 2002. Its broad catalog and variety of products in entertainment gives it an impressionable edge. Customers can shop anything from books to games, computers and TVs.

Part of what makes Takealot an e-commerce success story is that the online retailer strives to provide its customers with the very latest products in the market, coupled with up-to-date product specification.

In April 2017, Takealot scored a significant investment of over US \$69 million from Naspers, one of Africa's biggest digital companies. This came after the online retailer received US \$100 million investment from investment firm Tiger Global Management in 2014. Naspers boasts a 53,5% stake in Takealot, while Tiger Global owns about 34%.

KILIMALL

Kenya's largest online shopping mall, Kilimall is relatively new in the e-commerce space but has remarkably managed to create an inter-continental mark since its launch in 2014. The site, now established in other countries such as Nigeria and Uganda, has a retail customer base that continues to boom.

Kilimall is known for providing electronics such as phones, computers and gadgets, stocking top brands such Samsung, Huawei, Lenovo, and Phillips. The site also offers other products such as

home appliances, clothes, books, health and beauty products, and more. All its services are accompanied by a 7-day free return policy on their premium range of goods, making it an attractive choice for consumers.

KONGA

Konga has come a long way since its humble beginnings in 2012 as a Lagos-only e-commerce site that specializes in baby and beauty care. The online platform has morphed into a major online retailer, often dubbed “The Amazon of Africa.” In 2015, Konga joined forces with leading Nigerian banks to launch KongaPay, a safe and convenient online payment method to tackle the issue of trust in Africa when it came to online payments.

The online marketplace was one of the first in Africa to create a system of payment that was integrated with world banks – an innovation that uses a click system that eliminates the sharing of sensitive information during payments. With a backing from the South African media giant, Naspers, Konga is now a major player in the e-commerce space. In 2014, Naspers, which has a 50% stake in Konga, invested US \$50 million in the online store.

Customer Experience, Automation, AI

Ecommerce automation is software built to convert tasks, processes, or campaigns within your business to automations that intelligently execute exactly when needed. It’s how businesses can do more with what they have. It is about giving your people and yourself the most important thing you can: time. More than that, it unleashes your teams to invest in high value work in our current climate: retraining staff on new fulfillment processes, crisis communications, working out new deals with suppliers, dealing with HR challenges, experimentation, sales and marketing, and product iteration. Automating your eCommerce business is the key to taking much of that weight off your shoulders. With eCommerce automation, you can streamline the repetitive or mundane parts of your business that would otherwise start to consume too much of your time. Ecommerce automations can take a host of different forms like tagging customers for segmentation and marketing, standardizing visual merchandising, streamlining tracking and

reporting, and halting high-risk orders. With each workflow, the goal is the same: to simplify tasks.

Below are some examples of reduced manual tasks:

- Fulfilments: When an item is ready to be in store, trigger an email or SMS or Facebook message to the customer
- Inventory levels: Unpublish out-of-stock products and send a Slack message or email to your marketing team so they can pause advertising.

AI in e-commerce

With AI, eCommerce businesses can automate everything from featuring new products on multiple channels to synchronizing sales, identifying high-risk transactions, offering discounts to loyal customers, etc. Additionally, shifting the burden of answering routine queries to automated chatbots allows eCommerce business owners to focus on more complicated requests.

With the help of AI computer vision, an eCommerce business can identify the behavioral pattern of every customer on the basis of sales generated and the most viewed or purchased items. This data can be used later to attract them back to your eCommerce website. Push notifications are the most powerful retargeting strategy here. These notifications are brief and straightforward, so there's little risk of customers getting annoyed. An eCommerce business can also use personalized push notifications that provide one-on-one communication.

AI plays an enormous role in adding better customer experiences and innovative solutions in the eCommerce industry. Product recommendations, personalized shopping experiences, virtual assistants, chatbots, and voice search are some of the most distinctive uses of AI in eCommerce.

The advantages of gaining insights from customer data collection and then breaking it down can be further enhanced with AI to tailor online merchandising services to the interests and tastes of every customer.

With the help of AI and data collected from customers and businesses, today's eCommerce businesses make informed decisions by using that data more efficiently to forecast future results and adjust their marketing campaigns accordingly.

Benefits of Using Artificial Intelligence in Ecommerce Companies

1. More targeted marketing and advertising.
2. Increased customer retention
3. Seamless automation.
4. Efficient sales process.

AI Use Cases in Ecommerce

- Personalized product recommendations.
- Pricing optimization.
- Enhanced customer service.
- Customer segmentation.
- Smart logistics.
- Sales and demand forecasting.

How to Implement Artificial Intelligence into Ecommerce

1. Create a strategy.
2. Find narrow use cases that are relevant to the overall corporate strategy.
3. Leverage third-party expertise.
4. Build a full-scale solution.

Competition in the Market/ business mod (Competing against retailers and manufacturers)

Prior to the Competition Amendment Act 2018 (the Amendment Act), the public interest grounds specified in the Competition Act included the effect on the ability of small businesses or firms controlled by historically disadvantaged persons to become competitive. The Competition Act prohibits mergers likely to substantially prevent or lessen competition, unless outweighed by

technological efficiency or other pro-competitive gain or justified on certain public interest grounds. Uniquely, a merger could be prohibited or conditioned if, for example, it had a negative effect on the ability of firms controlled by historically disadvantaged persons to become competitive, whether it is anticompetitive or not. South Africa has been the leading jurisdiction in advocating a competition regulation regime that is concerned with not only efficiency of markets but also equity goals to address inequities in the distribution of opportunity. The public interest path adopted by South Africa has not been without critics (Griffiths & Gumbie, 2015) but, in the main, there is broad acknowledgement that the South African merger-control regime has ensured mergers do not yield adverse socio-economic outcomes that could perpetuate inequality, unemployment and poverty (Njisane & Ratshisusu, 2017 and Raslan, 2016). In this section, we look at black empowerment and its application in merger analysis. To do so, we focus on several interesting cases. The cases are chosen to span a range of substantive issues and to highlight choices that offer illustrative guidance.

The Competition Act prohibits agreements and decisions that constitute restrictive practices. Hard core cartels¹⁸ are prohibited per se. The Competition Act prohibits abuse of dominance practices aimed at excluding rivals or exploiting consumers. The system of prohibitions relating to abuse of dominance practices, horizontal and vertical restraints is balanced by an arrangement for exemptions. An exemption gives permission for applicants granted an exemption to contravene specific sections of the Competition Act. The Commission may grant an exemption for a specified term. On public interest exemptions, prior to the Amendment Act, the grounds for exemption included (1) maintenance or promotion of exports; and (2) promotion of the ability of small businesses or firms controlled by historically disadvantaged persons to become competitive. In deciding whether or not to grant an exemption, the Commission must establish whether the restrictive practice, for which an exemption is sought, is required to achieve the public interest objective and whether allowing firms to engage in the restrictive practice will contribute to the public interest objective.

Delivery (Reliable & Fast shipping and Sustainability)

The courier prices in South Africa will depend on the size of the parcel and the area you are delivering to. For rural areas, Pargo and Fastway are great options for cheap courier services. For standard size and destination, pricing is comparable between companies. Quality of service and convenience will be better criteria to choose between them.

Even if you want the cheapest courier service, it is important to review other factors when selecting your courier partner. For instance, having timely deliveries without damage to your parcels is crucial. Indeed, saving a few Rand on the shipping, but having to replace a lost or damaged parcel can lead to a significant loss.

Finally, to get the best prices, always remember to negotiate the rates with your courier service regularly. To do that, you need to start building a history with them. After some time, you can contact them to discuss the rates and see if they can bring down your pricing. They will often be happy to offer special rates.

Fastway is a low-cost national courier distribution service across South Africa. Established in 1983 in New Zealand, Fastway Couriers is a globally franchised courier company. They currently have a presence in New Zealand, Australia, Ireland, and South Africa.

Pargo is a delivery company in South Africa that focuses on solving the challenges of last-mile distribution. They allow customers to send and receive parcels at pickup points located in retail stores across the country. Store partners include Caltex gas stations, Clicks, FNB, or Wellness Warehouse shops.

The Courier Guy is one of the leading courier companies in South Africa. The business started in 2000 and is now a worldwide courier company. They offer a full range of courier services, including express, overnight as well as international courier options.

Payment system)

South Africa's National Payment System (NPS) clears more than 350 billion rand a day. NPS requires not only interbank payments, but also the entire payment process. This includes all systems, mechanisms, institutions, procedures, rules and laws.

PASA (Payment Association of South Africa) Is the South African Reserve Bank (SARB) designated Payment Systems Administrator (PSMB, Payment System Management Body). It should be noted that PASA is a non-profit organization, unlike China's UnionPay and Nigeria's NIBSS. SARB has a lot of focus on the National Payment System (NPS), which can be seen in Vision 2025, such as security and robustness and risk reduction.

Regulatory and regulatory framework



1、 “The South African Reserve Bank Act (SARB Act) ” Empowers the Reserve Bank (_UU_ sarb) to oversee National Payment System (_UU_ nps) regulations and ensure their safety, robustness and efficiency.

2, issued in 1998 “The National Payment System Act (NPS Act) ” The SARB is authorized to designate a PSMB to organize, manage, and regulate participating members of the NPS. The current PASA is a SARB approved PSMB.

3) Legal basis for participation in a particular payment system in the context of PASA is Payment Clearing House (Payment Clearing House PCH) Agreement (Agreements) in. Members' specific types of transactions and the clearing rules applicable to each PCH (Clearing Rules), which forms a Participant Group (_UU_ pg). A PG will be responsible for one or more PCH protocols.

(4) PPG will be responsible for designating one or more PCH Systems Operators (PSO) for each PCHS, and PASA will authorize the PSOs to conduct interbank payment transactions. make Do the liquidation. Through a review of Service Level Agreements, SLAs Member Participants and the PSO will be further managed. Transactions cleared by the PSO eventually adopt SARB on Real Time Accounting System (Real Time Gross Settlement system , RTGS) Complete the settlement. South Africa's RTGS is called SAMOS (South Africa Multiple Options Settlement) 。

Note: South Africa has 19 PCH and PASA has 34 bank members.

Level 3: System operator (System Operators, SOs) 。 This layer is composed of payment service providers, which are either clearing participants or system operators (SO). In accordance

with Directive 2 of SARB 2007, an SO provides services in connection with payment instructions, i.e., provides electronic means of payment (including sending and / or receiving payment instructions) to two or more persons to enable those persons to complete payment or / and collection.

So should not be confused with PSO. PSO is used for clearing, while SO is the technology infrastructure that assists participants and / or payment service providers to send or receive transactions. PASA stands for SARB and Authorising SO in accordance with SARB 2007 Directive 1.

Level 4: Third Party Payment Service (Third Party Payment Providers , TPPPs) 。 This layer consists of clearing participants and registered non-bank third-party payment service providers. There are two types of TPPS: Beneficiary Service Providers , and Payer Service providers. Under Directive 1 of SARB 2007, the PSP or BSP receives money or processes payment orders from two or more paying parties in order to complete payment due to third parties (Article 7 of the NPS Act).

TPP usually Provided by SO, it can be found in Limited time within Will receive the accounts payable to its bank account. And SO can only provide technology, but cannot place funds received from another party into its own bank account. All TPPs are required to register with PASS through a clearing participant.

Level 5: Users, Enterprises, Retail. Banks / TPPP / SO confirm their participation thresholds and align them with PCH rules and protocols.

Note: There are currently 88 SOs and 214 TPPPs.

Type of payment

There are many payment methods in South Africa, which can be divided into credit payment and debit payment.

Credit payment A credit payment (or credit push) is when a payer sends an order to the payer's bank to make a direct payment, which routes the order to a payee's bank and transfers the funds to the recipient's account.

This type of payment method is: periodic electronic payment (EFT Credit), periodic payment (Stop / Standing Order) 、 Real-time payments (_UU_ rtc Payment), domestic money transfers (_U_ domestic Money Transfer), cross-border remittances (_U_ cross Border

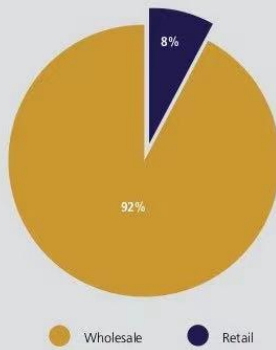
Remittance), high-value payments (U_ high Value Payment, Note: More than 5 million rand is a large amount.

Debit payment (debit payment, or debit pull) corresponds to a credit payment, Is the payer to the payee an authorization (mandate), and then the recipient submits the payment instruction to the recipient bank, then the payment order is sent to the paying bank, and the payor bank transfers the required funds to the receiving bank. Debit payment, The flow of funds and payment instructions in the opposite direction.

This type of payment method is: withholding (EFT Debit / Debit Order) 、 Early Debit Order (EDO), which is further divided into Authenticated and Non-Authenticated, Namely AEDO and NAEDO), ATM transactions, Self Service Devices (SSDs), Card Based Payment.

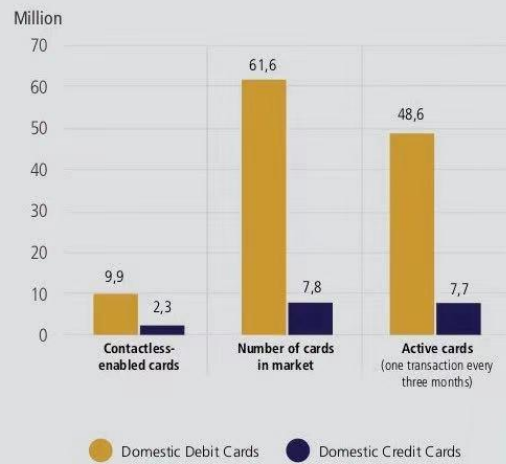
2018 trading data

2018 Split in settlement values*



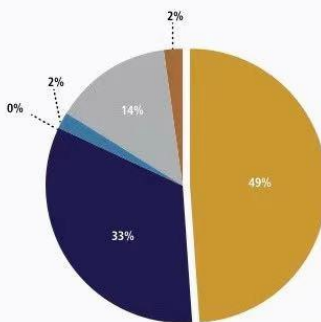
Card statistics*

1 January 2018 to 31 December 2018

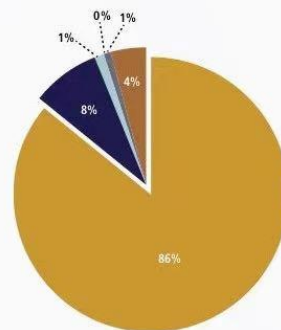


Retail

2018 Volumes*

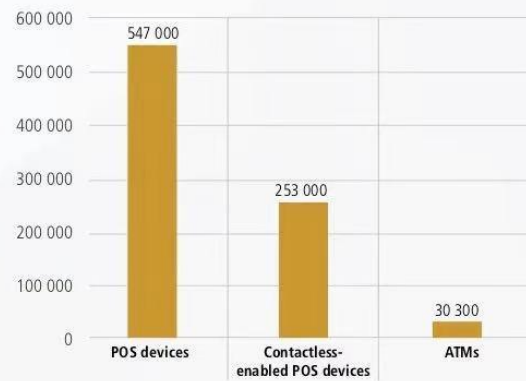


2018 Values*

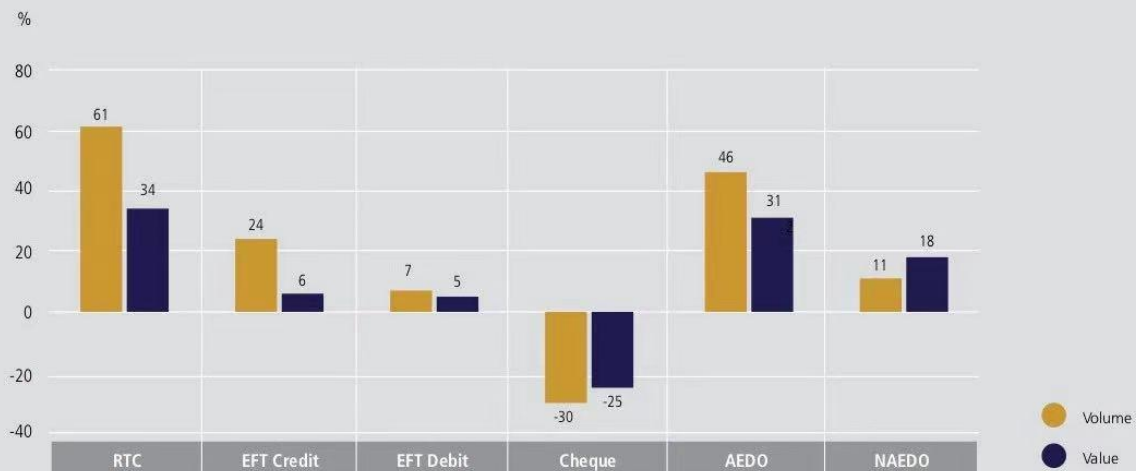


* Data sourced from BankservAfrica, Mastercard and Visa

Acceptance devices in market*

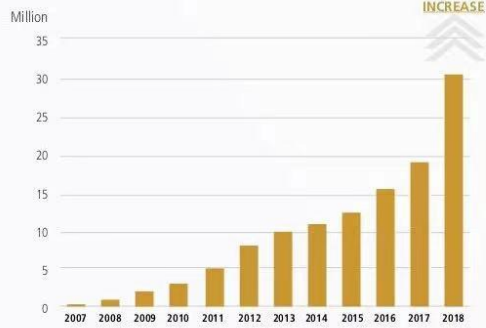


2018 year-on-year change*

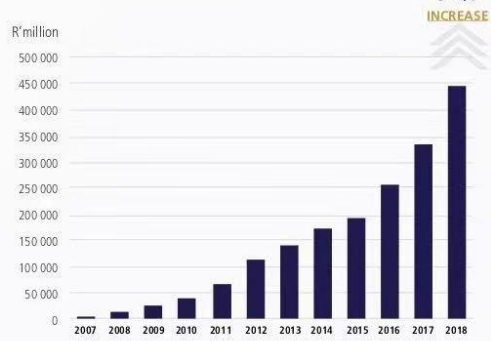


* Data sourced from BankservAfrica, Mastercard and Visa

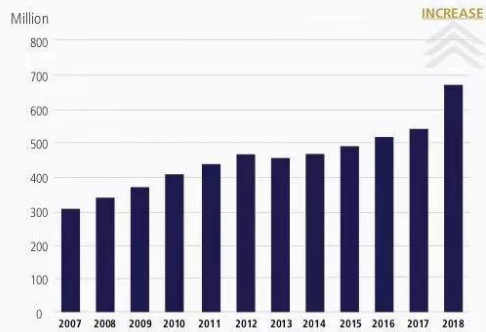
Real-time clearing volumes*



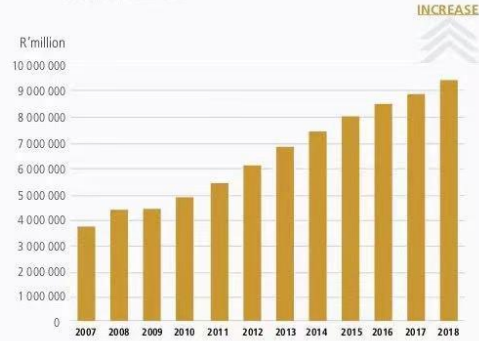
Real-time clearing values*



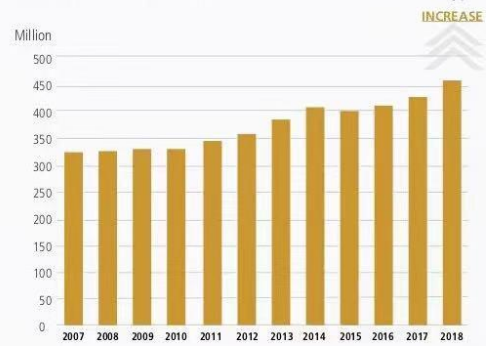
EFT credit volumes*



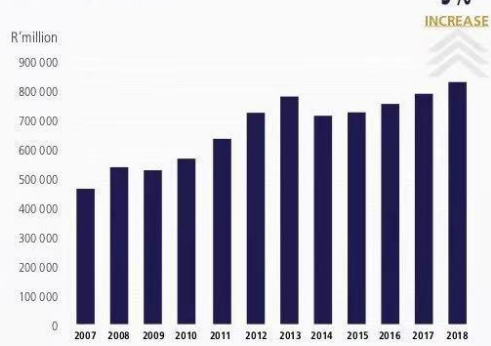
EFT credit values*



EFT debit volumes*

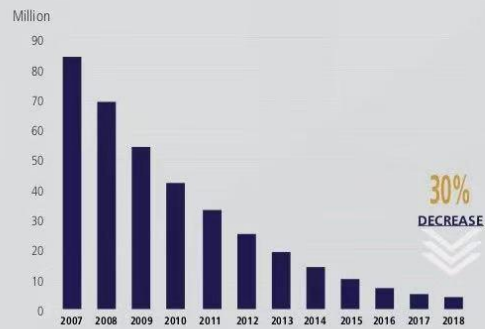


EFT debit values*

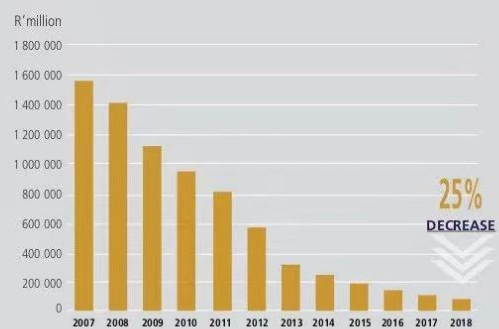


* Data sourced from BankservAfrica

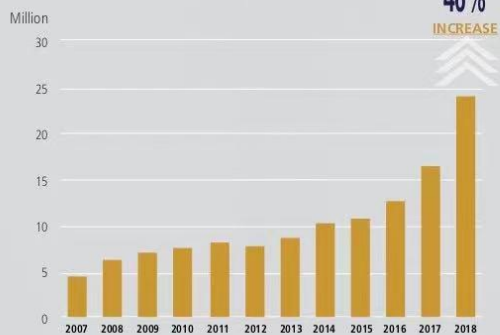
Cheque volumes*



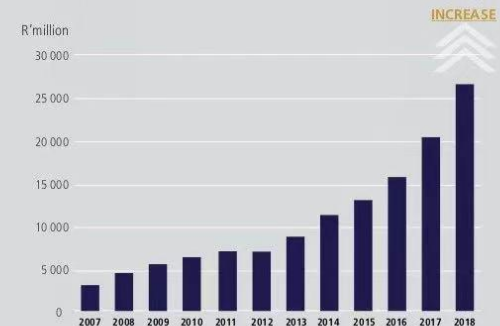
Cheque values*



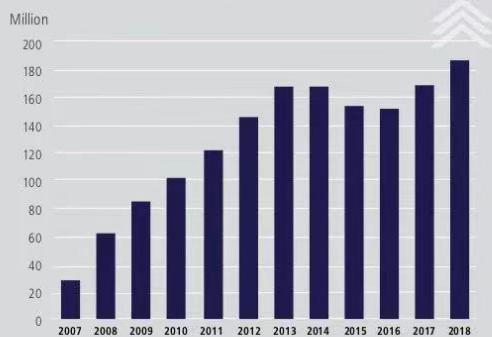
AEDO volumes*



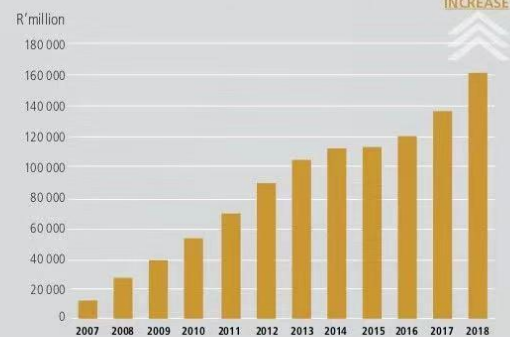
AEDO values*



NAEDO volumes*



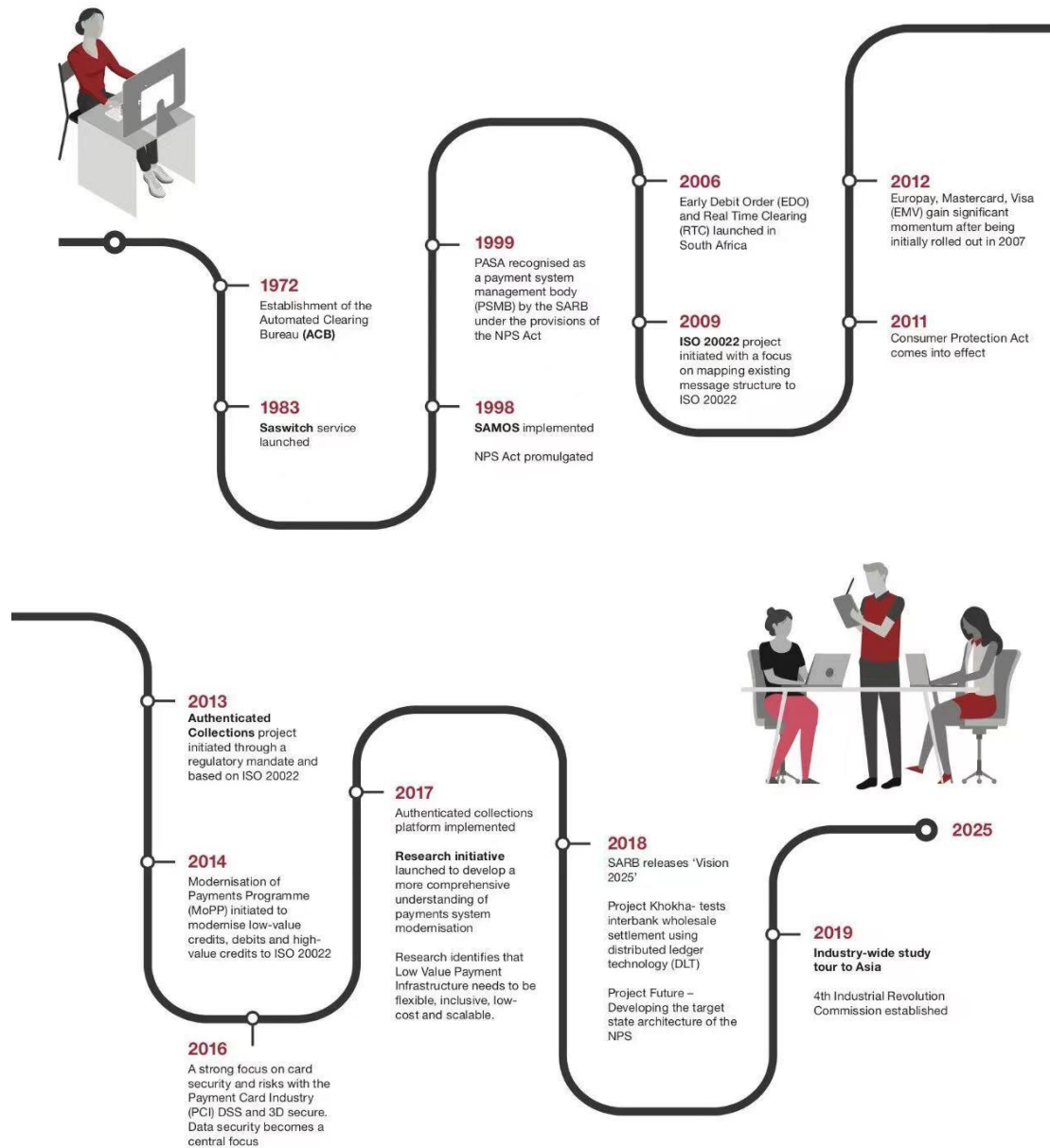
NAEDO values*



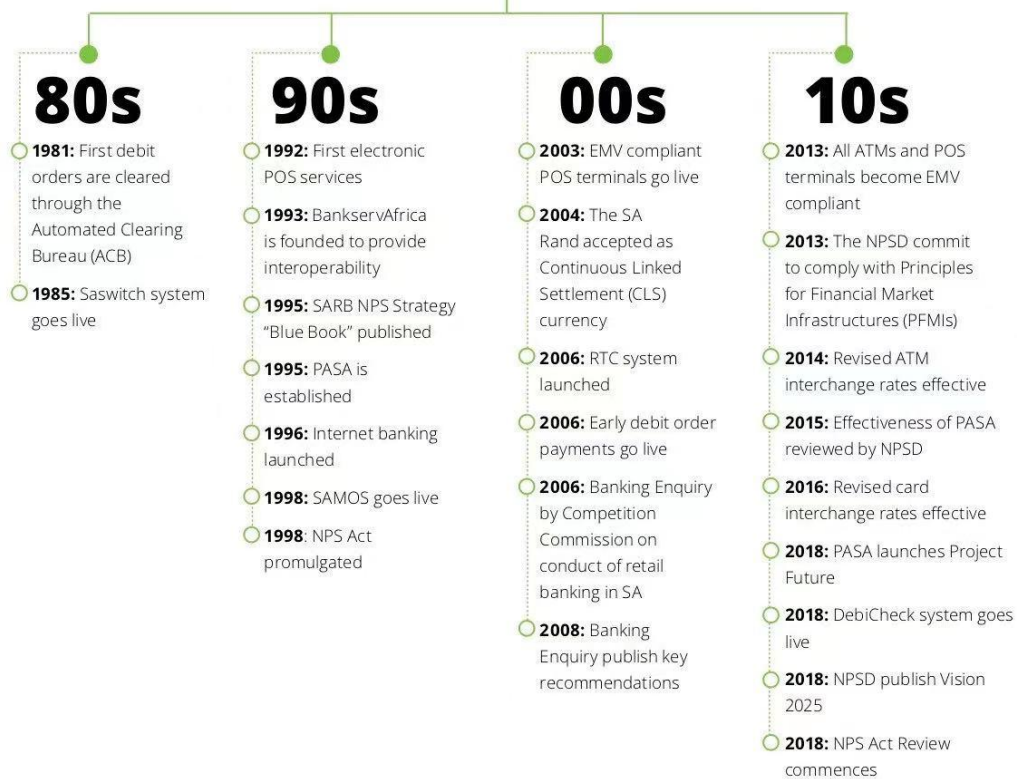
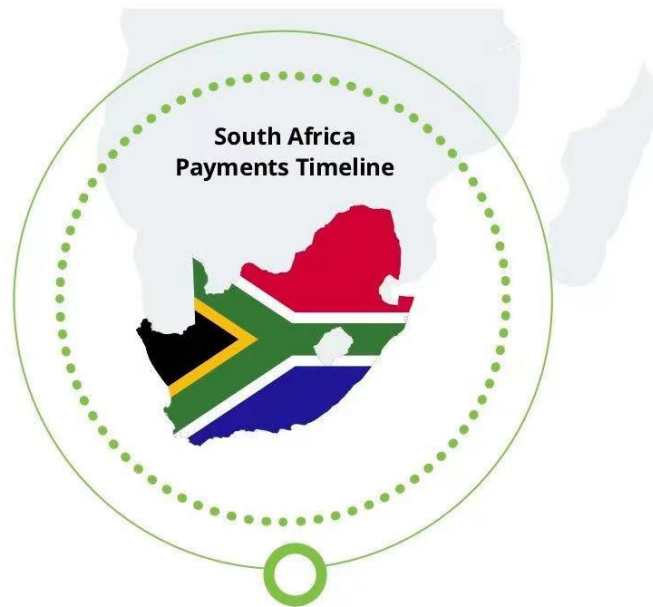
* Data sourced from BankservAfrica

Part1:Payment Modernization in South Africa

South Africa's modernisation journey



Attached 2:South Africa Payment Timeline



Ecommerce security & fraud prevention,data protection

What is Ecommerce Fraud?

Before you can protect yourself against ecommerce fraud, you need to understand what it is. So, let's define our terms. When we talk about ecommerce, of course, we're talking about commercial transactions conducted electronically over the Internet, typically through an online store. These transactions are usually made from desktop computers, laptops, tablets, and phones. When we talk about fraud, we're talking about criminal deception intended to result in financial or personal gain. Ecommerce fraud, then, is criminal deception conducted during a commercial transaction over the Internet with the goal of financial or personal gain of the fraudster while negatively affecting the bottom line of the merchant. Ecommerce fraud is also called payment fraud. Two things to remember about ecommerce fraud are that the target is an online merchant and the deception is intended to remain undiscovered.

Why Does Ecommerce Fraud Take Place?

Online payment fraud takes place for several reasons, some of them historical, some of them geographical and some of them legal.

1. Ease.

Before the Internet, fraudsters generally had to steal physical credit cards and make purchases with them. Breaking into homes and cars and robbing people on the street with the aim of obtaining credit cards was a risky business in itself. Occasionally, fraudsters were lucky enough to obtain credit card slips that a store had carelessly discarded and would use those card numbers to fraudulently order merchandise over the phone.

Today, fraudsters have it much easier. They simply visit a website on the dark web and buy as many stolen credit cards as they need. During the first half of 2019, there were at least 23 million stolen credit cards for sale on the dark web.

2. Anonymity.

Payment fraud is also popular because it is conducted unseen. The fraudsters don't have to walk into a store, say a word to anyone, or risk getting captured on store cameras. All they need is a computer and an Internet connection. They can operate from any location, at any time of day, unseen.

Online fraudsters typically create fake email accounts and rent post office boxes using aliases that reveal no personally identifiable information about themselves.

3. Evasion.

Ecommerce fraudsters know that police departments do not make ecommerce fraud a priority. For one thing, the amounts of money involved in each fraudulent transaction are typically small relative to other types of crimes. Plus, online fraud is increasingly conducted across international borders, making it hard for the police to locate and prosecute online criminals in other countries.

Six Types of Ecommerce Fraud

When you hear the term "ecommerce fraud," you likely think of stolen credit cards being used by criminals to buy products from online stores. But credit card fraud is just one of the most common types of fraud. Here are the top six.

1. Credit card fraud.

Credit card fraud is the umbrella term for fraud that is committed using a credit card or debit card. In the context of ecommerce fraud, credit card fraud is also known as card-not-present fraud and payment fraud. In credit card fraud conducted online, the fraudster uses stolen credit card information to purchase products or services from a web merchant.

In a typical scenario, a criminal visits a site on the dark web that sells stolen credit cards. The criminal buys the card data and visits an online store, using that stolen card number to buy a

product or service. This initial transaction defrauds the cardholder whose card was stolen. But eventually it defrauds the store owner, who must refund the purchase (and sometimes pay a chargeback fee to the bank that issued the card). Merchants can also become victims to card testing scams, where multiple credit cards are attempted to test which are still active and will allow for purchases. These types of purchases are usually small, low-risk orders, but can add up to a big hit on a merchant's bottom line.

2. Affiliate fraud.

Affiliate fraud is illegal activity intended to generate affiliate commissions. In affiliate marketing, online merchants pay affiliates a commission for sales that affiliates refer to. The merchants give affiliates a unique, trackable web link that points shoppers to the merchant's store pages. When a shopper clicks on one of these links and makes a purchase, the merchant rewards the affiliate for the referral by giving the affiliate a commission (typically a percentage of the sale price).

In affiliate fraud, criminals game the system and defraud the online merchant using fake activity to either generate commissions or to increase the amount of the commissions.

A common form of affiliate fraud is "typosquatting," in which a criminal registers domain names that match commonly mistyped versions of an online store's legitimate URL. The fraudster then redirects that domain name to the merchant's website—but with an affiliate link.

3. Chargeback fraud.

In the world of credit card transactions, a chargeback is a demand that a credit card provider makes to a retailer to refund a fraudulent or disputed transaction.

In the online commerce world, chargeback fraud occurs when an online shopper makes a purchase with their credit card, receives the purchased goods or services, but then requests a refund from the credit card company, who pushes that through the issuing bank (the bank that issued their credit card, also known as the card issuer). Commonly referred to as "friendly fraud," this type of fraud results in the payment processor demanding that the retailer refund the

purchase amount to the issuing bank. When a bank demands a chargeback, the online merchant is responsible for refunding the purchase.

In a typical scenario of chargeback fraud, a shopper makes a purchase from an online store. After receiving delivery of the goods or services, the criminal waits weeks or months, then contacts their bank and disputes the transaction, claiming it to be unauthorized or fraudulent. The fraudster hopes that the merchant lacks the time and resources to dispute the claim, or simply gives them the benefit of the doubt.

4. Phishing/account takeover.

Most ecommerce stores provide customers with accounts that store personal information, financial data, and purchase history. Cybercriminals hack into these accounts through phishing schemes. In one of the most common tactics, fraudsters send emails to trick customers into revealing personal data like usernames and passwords. They then log into the customers' accounts, change the passwords, and make unauthorized purchases. Social media logins are a common way that shoppers can create accounts easily on ecommerce sites, but if that information is hacked, it can be devastating. Criminals are also using bots to steal confidential information, resulting in customers being plagued by the fallout of identity theft.

5. Interception fraud.

In interception fraud, fraudsters use stolen credit cards to make online purchases, ship the goods to the address that's on file for the credit card at checkout, but then intercept the package before it is delivered. For example, a criminal will visit an online merchant such as Amazon and use a stolen name, address, and credit card to purchase an item. After the transaction is completed, the criminal calls customer service before the item has shipped and changes the delivery address to the criminal's desired pickup location.

6. Triangulation fraud.

Triangulation fraud uses three steps to defraud online merchants. In the first step, criminals create a fake online storefront, typically one that offers popular brand-name goods at bargain-basement prices. The only goal of the site is to steal names, addresses and credit card numbers from unsuspecting shoppers.

In the second step, the fraudsters use the stolen customer credentials and credit card numbers to visit a legitimate online store, buy exactly what the victim purchased from the fake store, and ship it to the customer.

The third step is the payoff for the fraudsters. They use the stolen customer data to make additional online purchases that they ship to themselves. This type of fraud typically remains undiscovered for a longer time than other types of online fraud because the original purchase (from the fake site) raises no suspicions on the part of the victim.

How to Identify Ecommerce Fraud Online

As an online merchant, you can spot ecommerce fraud in a number of ways. Just remember that the success of ecommerce fraud depends on the skill and ingenuity of the fraudsters. As merchants increase their defenses against online criminal activity, online crooks also up their game and devise cunning ways to defraud their targets. Here are the most common red flags to look for:

- Inconsistent order data: The zip code and city entered don't match. Or the IP address of the shopper and their email address don't match.
- Larger than average order: The order is far larger than your customer typically spends. Other red flags include multiple units of the same SKU in one order, and expedited shipping (the crook wants to receive the order before getting caught).

- Unusual location: Your customer always purchases from an IP address in North America but suddenly makes a purchase from an IP address in an unusual location (Nigeria, for example).
- Multiple shipping addresses: The buyer makes multiple purchases under one billing address but ships the products to multiple addresses.
- Many transactions in a short timeframe: The fraudster makes multiple purchases back to back—and it's not the holiday season.
- Multiple orders from many credit cards: Someone makes multiple purchases using multiple credit cards (either in one day or over a longer period).
- Multiple declined transactions in a row: The purchaser makes not just one or two attempts (honest shoppers make mistakes, after all), but four, five, six, seven, eight or more attempts without getting the card number, expiry date, and card security code correct.
- Strings of orders from a new country: You've never received a single order from the Kingdom of Bhutan, and then you suddenly receive 11 orders from that country in the space of a week.

Solutions

The key to protecting your online store from fraudulent credit card transactions, affiliate fraud and other types of ecommerce fraud isn't just recognizing these activities when you see them—it's taking preventative measures that will reduce your fraud risk in the first place.

1. Conduct regular site security audits.

Want to discover flaws in your security before criminals and fraudsters do? Conduct security audits—often. Ask yourself these questions:

- Are our shopping-cart software and plugins up-to-date?
- Is our SSL certificate current and working?

- Is our store PCI-DSS compliant (Payment Card Industry Data Security Standard)?
- Are we backing up our online store often enough?
- Are we using strong passwords for admin accounts, hosting dashboards, CMS, database, and FTP access?
- Are we scanning our website regularly for malware?
- Are we encrypting communication between our store and our customers and suppliers?
- Have we removed inactive plugins?

2. Make sure your store is PCI compliant.

If you operate an online store that accepts credit card payments, you must be PCI compliant. PCI stands for Payment Card Industry. PCI standards for compliance are developed and managed by the PCI Security Standards Council to ensure the security of credit card transactions in the payments industry. PCI compliance means your online store and your business processes meet these PCI standards. If you operate a SaaS-based ecommerce store, your platform will typically provide this compliance.

3. Monitor your site regularly for suspicious activity.

Bricks-and-mortar stores hire fraud prevention officers to catch shoplifters. You can protect your online store against fraudulent transactions by monitoring your store for suspicious activity. Monitor your accounts and transactions for red flags, such as inconsistent billing and shipping information, as well as the physical location of your customers. Use tools that track customer IP addresses and alert you to any addresses from countries known as a base for fraudsters.

4. Use an Address Verification Service (AVS).

Credit card processors and issuing banks will usually offer an Address Verification Service to detect suspicious credit card transactions in real-time and prevent credit card fraud. The Address Verification Service checks the billing address submitted by the card user (the customer) with the cardholder's billing address that's on file with the issuing bank. This check takes place as part of the merchant's request to the payment processor for authorization of the credit card transaction.

When addresses don't match, the system either declines the transaction or flags it for investigation.

5. Require Card Verification Value (CVV) numbers for all purchases.

The three-digit security code on the back of VISA®, MasterCard® and Discover® credit and debit cards and the four-digit security code on the back of American Express® credit and debit cards is called the Card Verification Value (CVV) or Card Security Code (CSC). By requiring all purchasers to supply this code for every transaction, you ensure that customers have the physical credit card in their possession. This helps to keep you safe and reduces fraud.

6. Use Hypertext Transfer Protocol Secure (HTTPS).

HTTPS is the secure version of HTTP, which is the primary protocol used to send data between a customer's web browser (like google) and your online store. HTTPS encrypts this data to protect sensitive information, such as customer names, addresses and credit card numbers. Using HTTPS prevents your online store from having its transactions broadcast in a way that's easily viewed by hackers, cybercriminals, and fraudsters. You use HTTPS by buying an SSL certificate.

7. Avoid collecting too much sensitive customer data.

One way to protect your store in the event of a data breach or hack is to collect and store as little customer data as possible. Hackers can't steal what you don't have. So only collect the data you need to complete a transaction and ship the product. Avoid collecting Social Security numbers, birth dates and other unnecessary sensitive customer data.

8. Set limits on purchases.

Based on your order and revenue trends, set limits for the number of purchases and total dollar value you'll accept from one account in a single day. This reduces your exposure to a minimum should fraud occur.

9. Try an anti-fraud solution.

When it comes to detecting and preventing online fraud, there are a variety of software solutions to suit your needs and your budget. Additionally, the tools you select may vary widely when it comes to how much work is involved in installation and ongoing management. Some may prefer a more hands-on solution, while others would rather leave it in expert hands.

- Rudimentary anti-fraud tools perform a specific, single function. They are typically integrated into online shopping carts and ecommerce platforms. These tools use machine learning algorithms to identify fraudulent transactions through IP geolocation, validate email addresses, conduct device fingerprinting, and verify addresses.
- Mid-level anti-fraud tools offer a wider variety of functions, including chargeback guarantees, auto declining of high-risk orders, protections against new account fraud and account takeover protection.
- Top-level anti-fraud tools offer everything the other tools offer plus outsourced case management, expertise working with large merchants, loyalty fraud management, policy abuse protection, automatic decisions, and manual review of suspicious transactions, ensuring that no good order is mistakenly declined by the software.

10. Double check that the IP address and credit card address match.

Every order placed on your online store comes from a unique, public IP address (a string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over the Internet). From the IP address, you can generally detect the city or region of the world where the purchaser is making the purchase. If this city or region does not match the address of the credit card being used, that's a red flag.

11. Avoid non-physical shipping addresses.

Fraudsters commonly avoid detection by protecting their physical address, preferring to use a PO box or other anonymous location. After all, the police can't come knocking if there's no door to knock on.

If you are an online merchant, and if you want to prevent this type of fraud, never ship online orders to PO boxes and other virtual addresses, such as those of freight forwarders. You can spot addresses that belong to freight forwarders because they have a container number in the address, such as 726 Dock Road Suite 300 #KXQ-582899328.