

Anatomy of Fraud Report 2023

Assessing the Magnitude of Fraud and
Countering Risks with Mitigation Strategies



 Bureau



 PRAXIS
GLOBAL ALLIANCE

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

FDP market landscape in Southeast Asia

FDP playbook

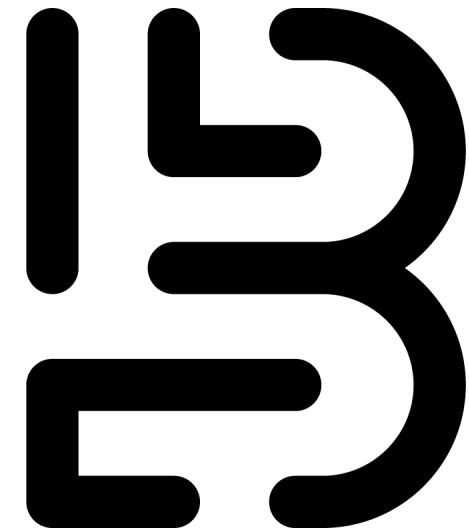
Appendix

Introduction

As businesses continue to operate in an increasingly globalised and technologically advanced world, the risks associated with fraud are growing. Geopolitical and economic factors, combined with the ever-increasing sophistication of fraudsters, have made it difficult for organisations to protect themselves against various types of fraud, such as synthetic identities, bot attacks and account takeovers, to name a few. The consequences of falling victim to fraud can be severe, not only in terms of financial losses but also damage to a company's reputation. Indeed, when creating new accounts, approximately 9% of instances are associated with fraudulent activities. From July to December 2021 alone, a staggering 130 million fraudulent incidents were recorded during account logins. These numbers highlight a pressing necessity for implementing enhanced security measures. To stay ahead of the curve, businesses must keep up with the latest trends and best practices for fraud detection and prevention.

To this effect, Bureau conducted a survey to study the impact of digital fraud globally, especially in India and Southeast Asia (SEA), to address the increasing significance of fraud detection and prevention (FDP) solutions in the global marketplace. This report provides a comprehensive analysis of the FDP market globally and regionally, highlighting the latest trends and best practices for fraud detection and prevention.

Praxis Global Alliance, a top research and consulting firm, collaborated with the Bureau to provide critical insights for businesses seeking to manage digital fraud risks effectively. The report highlights the growing need for FDP solutions, with the global FDP market expected to reach US\$ 86B by 2027 and 60% of organisations planning to increase their FDP budget in the next two years. FDP solutions can reduce fraud operational costs, false positives, and chargebacks, facilitating real-time monitoring, seamless CX, and orchestration capabilities, eliminating white spaces across various industries. Investing in FDP solutions can lead to potential benefits such as cost reduction, improved user experience, and better orchestration capabilities, enabling businesses to make informed decisions and protect their financial and reputational interests.



Glossary

	Acronym	Description	Acronym	Description	Acronym	Description
Industry related	AML	Anti money laundering	CTS	Cheque truncation system	NACH	National automated clearing house
	AMLS	Anti money laundering suite	CX	Customer experience	NEFT	National electronic funds transfer
	APAC	Asia-Pacific	D2C	Direct-to-consumer	NFC	Near field communication
	API	Application programming interface	DLA	Digital lending applications	NFT	Non-fungible tokens
	AR	Augmented reality	DOS	Denial of service	NPS	Net promoter score
	ARPA	Average revenue per account	FDP	Fraud detection and prevention	OCR	Optical character recognition
	ARR	Annual recurring revenue	FMR	Fraud monitoring return	OTP	One-time password
	ATO	Account takeover fraud	FS	Financial services	POC	Proof of concept
	B2B	Business-to-business	GTM	Go-to-market	RBI	Reserve bank India
	B2C	Business-to-consumer	IDV	Identity verification	ROI	Return on Investment
	BD	Business development	IFP	Intelligent forms processing	RTO	Return to origin
	BEC	Business email compromise	IMPS	Immediate payment service	SaaS	Software as a service
	BFSI	Banking, financial services and insurance sector	IOT	Internet of things	SEA	Southeast Asia
	BGV	Background verification	IP	Internet protocol	SEO	Search engine optimization
	BNPL	Buy now, pay later	IRDAI	Insurance regulatory and development authority of India	TAM	Total addressable market
	BSA	Bank secrecy act	KYC	Know your customer	TAT	Turn around time
	CAC	Customer acquisition cost	L&D	Learning and development	TPA	Third party administrators
	CFR	Central fraud registry	LTV	Life time value	UI / UX	User interface / user experience
	CPL	Cost per lead	MCA	Ministry of corporate affairs	UPI	Unified payments interface
	CSAT	Customer satisfaction	MRR	Monthly recurring revenue	VR	Virtual reality
Units	B	Billion	INR	Indian rupee	QOQ	Quarter on quarter
	CAGR	Compound annual growth rate	M	Million	YOY	Year on year
	CY	Calendar year	T	Trillion		
	FY	Financial year	US \$	United States dollar		

Highlights of the Global FDP market

31B+

FDP TAM, 2022 (US\$)

~22%

FDP TAM CAGR, 2022 - 27

86B+

FDP TAM, 2027 (US\$)

~58%

BFSI share in FDP TAM, 2022

~22%

E-commerce share in FDP TAM, 2022

~69%

Internet penetration, 2022

Source(s): ACI Worldwide, Industry reports, Press release, Praxis analysis

Executive summary: Global FDP landscape

- There are a variety of fraud like bot attacks, website cloning, mule accounts, among others that are **present across sectors**, whereas **certain fraud are industry-specific** like KYC fraud (BFSI), delivery fraud (e-commerce) etc.
- **FDP solutions help enterprises in reducing fraud operational costs, false positives and chargebacks pre and post – authorization.**
- Advancements in **AI and deep learning technologies** have strengthened the capabilities of FDP solutions.
- FDP solutions benefit all the participating stakeholders (user, FDP player, payment gateways, etc.) in an ecosystem of a digital transaction.
- **Budget constraints, poor / unstructured data quality** are the key headwinds for FDP players; growing digitalization, high in-house FDP costs are the key growth drivers.
- **60%** of organizations are expected to **increase their FDP budget** in the next two years as they look to **advance their automation and analytical capabilities** to fight fraud.
- **New-age SaaS FDP players** help organizations not only in **detecting fraud post occurrence** but also in **preventing fraud from occurring** by using advanced analytics → **reduced losses.**
- FDP buyers need solutions that can **balance user experience** with **robustness of fraud prevention.**
- The global FDP market stood at **US\$ 31B+ in 2022** and is expected to reach **~US\$ 86B in 2027**, growing at a **CAGR of 22%**; **APAC** is the **fastest-growing region.**
- FDP solutions enable seamless CX, orchestration capabilities, real-time monitoring etc., facilitating in the elimination of white spaces across industries.

Highlights of the India FDP market

1.5B+

FDP TAM, 2022 (US\$)

~37%

FDP TAM CAGR, 2022 - 27

7.6B+

FDP TAM, 2027 (US\$)

~73%

BFSI share in FDP TAM, 2022

~24%

E-commerce share in FDP TAM, 2022

~62%

Internet penetration, 2022

Source(s): Source(s): ACI Worldwide, Industry reports, Press release, Praxis analysis

Executive summary: Indian FDP landscape

- Total addressable FDP market was **US\$ 1.5B+** in 2022 and is projected to reach **US\$ 7.6B+** by 2027, growing at a CAGR of **37%**.
 - FDP SAM was **US\$ 570M+** in 2022 and is expected to cross **US\$ 3,152M** by 2027, growing at a CAGR of **41%**.
 - **BFSI constituted 70%+** of the total FDP addressable market in 2022 followed by **e-commerce (~24%)**.
 - Outsourced FDP services held **~35%** of FDP TAM in 2022 and are expected to **increase to 40% by 2027**.
- India to have **~1,144M internet users by 2027**, growing at a CAGR of **5%**; **62%** was the internet penetration in 2022 and is expected to be **~78%** by 2027.
- Government has **laid down various key regulations** like 2-factor authentication, KYC process, etc. to mitigate fraud that is expected to drive spend on FDP solutions.
- **Volume of digital transactions to be ~122B** and is expected to be **1.9T+** by 2027, growing at a CAGR of **~74%**; **growing digital commerce, increasing adoption of digital native products, and rising internet penetration** are the key factors driving digitalization.
- Enterprises in Banking and financial services, Insurance, and Gaming sectors typically develop in-house FDP solutions.
- **Frictionless CX with robust security, unavailability of quality data** are the key challenges faced by FDP players; factors such as **accelerating digitalization, an increasing number of fintech startups** are creating headroom for the growth of FDP players in India.
- **High fraud detection accuracy, real-time monitoring, and ease of integration** are the key criteria influencing the purchase of FDP solutions.

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

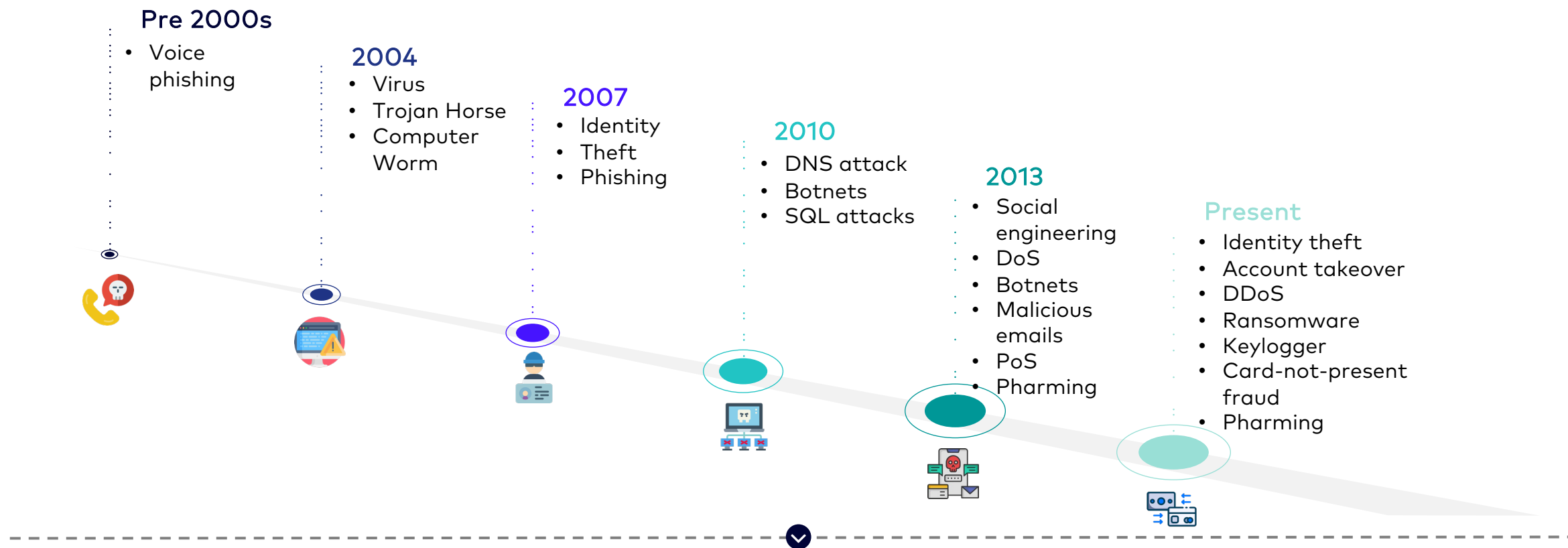
FDP market landscape in Southeast Asia

FDP playbook

Appendix

With advancements in technology, fraud has become more sophisticated nowadays; authentication processes are also evolving to detect and prevent fraud

Fraud is evolving rigorously from voice phishing to AI driven sophisticated and complex fraud



To combat and mitigate new complex fraud, advanced and strong authentication processes are being implemented by FDP players



Note(s): This is not the exhaustive list
Source(s): Industry reports, Secondary research, Praxis analysis

Digital fraud happens when an individual with malicious intent takes advantage of the various points of vulnerabilities across a digital transaction journey of a user

	Account opening	Login and Transaction	Post transaction
Verification methods to detect and prevent fraud	<ul style="list-style-type: none"> • Know-your-customer (KYC): Largely used by banks requiring verification of biometrics and identification documents including unique ids, permanent account numbers etc. • Additional verification of personal images and gestures for fintechs • Verification of emails and phone numbers for other industries including e-commerce 	<ul style="list-style-type: none"> • User verification based on passwords and one-time-passwords sent to the registered email ids or mobiles • Use of additional layer of authentication that requires the user to detect captcha, recognize images or solve a simple arithmetic problem 	<ul style="list-style-type: none"> • Verification sent to email ids of the purchase or transaction made • Regular updates sent to the user on email and phone to indicate the geo-position and status of delivery
Points of vulnerabilities	<ul style="list-style-type: none"> • Lack of awareness in sharing OTPs • Phishing emails or messages • Middlemen 	<ul style="list-style-type: none"> • Points of integration between the intermediary and payment platform • Third party payment merchants 	<ul style="list-style-type: none"> • Validation of intent • Failure in detection of collusion • Post facto alerts to merchant / buyer
Examples of fraud	<ul style="list-style-type: none"> • KYC fraud • Synthetic identity • Promo abuse 	<ul style="list-style-type: none"> • Account take over (ATO) • Promo abuse • Bot attacks • Social engineering fraud • Credit card fraud 	<ul style="list-style-type: none"> • Claims related fraud • Return fraud • Mule accounts • Unauthorized chargebacks

Source(s): Secondary research, Praxis analysis

Each vertical has several key types of fraud [1/3]

	Phases of journey	Fraud type	Brief description	Impact - volume of fraud	Impact - value of fraud
Banking and financial services	Account opening	KYC fraud	<ul style="list-style-type: none"> Fraudsters opening new accounts by either impersonating legitimate customers or using fake identities to gain access to an existing account 		
		Synthetic identity	<ul style="list-style-type: none"> Fabricated credentials where the implied identity is not associated with a real person 		
	Login and transaction	Website cloning	<ul style="list-style-type: none"> Cybercriminals create a 'clone' site of the original website and then send links to unsuspecting users via emails, text messages, social media posts 		
		Account takeovers	<ul style="list-style-type: none"> Scammers use phishing and hacking techniques to access users' accounts 		
		Social engineering	<ul style="list-style-type: none"> A fraudster gains the trust of an individual and 'tricks' them into sharing confidential information or even transferring funds directly to the criminal 		
	Post transaction	Bot attack	<ul style="list-style-type: none"> Bots mimic human interactions with web applications in an extraordinarily persuasive way making it difficult to detect and manage them 		
		Mule accounts	<ul style="list-style-type: none"> Criminals transfer stolen money on behalf of others, usually through their bank account 		
		Stolen / fake credit card	<ul style="list-style-type: none"> Scammers generate fake cards via credit card skimming where the scammer attaches a small device to the transaction machine that cannot be easily noticed 		
		Identity fraud	<ul style="list-style-type: none"> Involves the use of a person's stolen details to commit crime, typically associated with CNP* 		
		Fraudulent fund transfers	<ul style="list-style-type: none"> Fraudsters use an emulator or app cloners to make a bank transfer or top up an account 		
Insurance	Account opening	Intermediary fraud	<ul style="list-style-type: none"> Fraud perpetuated by an insurance agent / corporate agent / intermediary / third party administrators (TPAs) against the company and policyholders 		
	Login and transaction	Policyholder fraud	<ul style="list-style-type: none"> Fraud against the company in the purchase and / or execution of an insurance product 		
	Post-transaction	Claims related fraud	<ul style="list-style-type: none"> Hiding a pre-existing condition or duplicate bills of exchange Fabricated documents to meet terms and conditions of the insurance 		

Note(s): * Card not present. This is not the exhaustive list
 Source(s): Industry reports, Secondary research, Praxis analysis



Each vertical has several key types of fraud [2/3]

	Phases of journey	Fraud type	Brief description	Impact - volume of fraud	Impact - value of fraud
Retail and e-commerce	Login and transaction	Promo abuse	<ul style="list-style-type: none"> Occurs when an individual customer, vendor / agency takes advantage of a promotion, abusing the coupon policy 		
		Payment fraud	<ul style="list-style-type: none"> Any kind of illegal online transaction performed by a cybercriminal 		
	Post-transaction	Delivery fraud	<ul style="list-style-type: none"> Identity fraud <ul style="list-style-type: none"> Fraudster attempts to obtain personal user data via malware, fake websites, emails, etc. Uses these to purchase goods on an invoice and have them sent to a different delivery address Friendly fraud <ul style="list-style-type: none"> Customer himself does not intend to pay for the ordered goods and claims that they never arrived 		
		Return fraud	<ul style="list-style-type: none"> Receipt fraud: Using reused, stolen, or falsified online receipts to return merchandise for profit Price arbitrage: Purchasing differently priced but similar-looking merchandise and returning the cheaper item as the expensive one Switch fraud: Purchasing a working item, and returning a damaged or defective identical item Wardrobing: Buying a clothing item with the intention of wearing it for a short time and returning it later 		
Technology and internet	Login and transaction	Phishing and spoofing	<ul style="list-style-type: none"> Use of email / online messaging services to dupe victims into sharing personal data, login, and financial details 		
		Data breach	<ul style="list-style-type: none"> Stealing confidential, protected, or sensitive data from a secure location and moving it into an untrusted environment → data being stolen from users and organizations 		
		Denial of service (DoS)	<ul style="list-style-type: none"> Interrupting access of traffic to an online service, system, or network to cause malicious intent 		
		Malware	<ul style="list-style-type: none"> Use of malicious software to damage or disable users' devices or steal personal and sensitive data 		
		Ransomware	<ul style="list-style-type: none"> Prevents users from accessing critical data and then demanding payment in the promise of restoring access 		
		Business email compromise (BEC)	<ul style="list-style-type: none"> Sophisticated form of attack targeting businesses that frequently make wire payments Compromises legitimate email accounts through social engineering techniques 		

Note(s): This is not the exhaustive list
 Source(s): Industry reports, Secondary research, Praxis analysis






Each vertical has several key types of fraud [3/3]

	Phases of journey	Fraud type	Brief description	Impact - volume of fraud	Impact - value of fraud
Real money gaming	Account opening	Synthetic identity	<ul style="list-style-type: none"> Fraudsters create fake new accounts using synthetic identities or fake credentials and identity elements bought on the dark web 	●	●
	Login and transaction	Account takeover	<p>Commonly used ways in which fraudsters hack into gamer accounts include:</p> <ul style="list-style-type: none"> Creating spoof sites to steal login credentials. Buying user credentials on the dark web for credential stuffing. Phishing scams. Offering help or bonuses in-game in exchange for player credentials 	●	●
		Promo abuse	<ul style="list-style-type: none"> Fraudsters engage in promo abuse to test credit cards, create fake accounts, and hack existing accounts Fraudsters take advantage of sign-up bonuses or marketing promotions by creating new fake accounts Online games and gambling sites that offer US\$ 0 authorization fees are especially vulnerable to card testing 	●	●
		Bot attack	<ul style="list-style-type: none"> Fraudsters program bots to automate and increase the speed and velocity of card testing 	●	●
	Post - transaction	Friendly fraud	<ul style="list-style-type: none"> Games with in-app purchases or microtransactions are especially prone to friendly fraud 	●	●
Gig economy	Login and transaction	Account takeover	<ul style="list-style-type: none"> Fraudsters access stolen credentials for the purposes of accessing delivery service accounts 	●	●
		Phishing	<ul style="list-style-type: none"> Phishing attacks are quite prevalent, resulting in a wealth of stolen data for ATO attacks Fraudsters try to attract freelancers by posting fake job openings 	●	●
	Post - transaction	Pay to work	<ul style="list-style-type: none"> In this scam, freelancers are asked to send payment before being hired Fraudsters making individuals pay upfront to work for them earn a profit by signing people up 	●	●
		Money mules	<ul style="list-style-type: none"> One of the most common roles for a mule is in "parcel mule" scams. Fraudsters employ people to receive stolen goods, repackage them, and send them off to an address owned by the fraudster 	●	●

Note(s): This is not the exhaustive list
 Source(s): Industry reports, Secondary research, Praxis analysis



FDP solutions are technology platforms and tools that proactively monitor, alert and mitigate fraud across a digital transaction customer journey

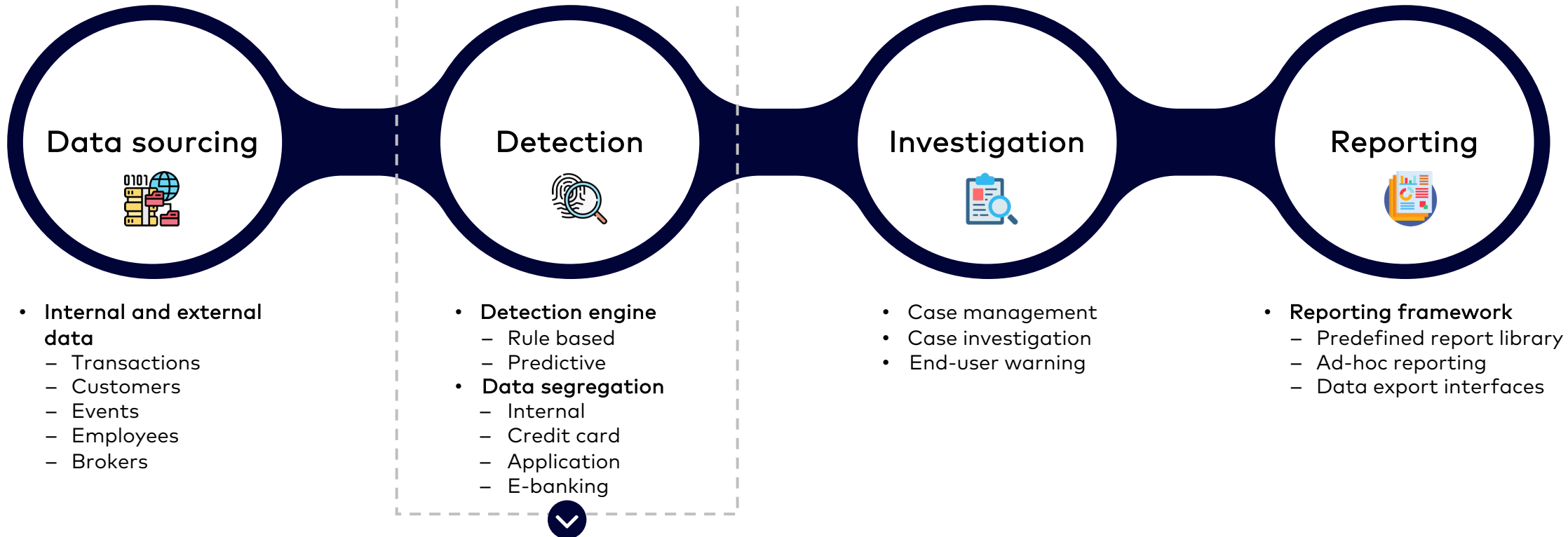
		Account opening	Login and Transaction	Post transaction
Current challenges 		<ul style="list-style-type: none"> Manual verification of identity proofs is time consuming and error prone Waiting period 2 to 7 days Multiple checks diminishes UX Multi-factor authentication may be cumbersome 	<ul style="list-style-type: none"> Multiple checks diminishes UX Multiple authentication is a challenge in case of numerous transactions Time taking process pushes users to switch to user friendly applications 	<ul style="list-style-type: none"> Majority authentication alerts on various forums like SMS, email, etc Calls for authenticating transactions can hamper customer sentiments Source and destination might be different for the same user account
FDP capabilities 		<ul style="list-style-type: none"> Verifies digital documents, gestures, images and video through advanced analytics and integration with databases and bureaus in real time Reduces the need for manual checks, multiple user touchpoints 	<ul style="list-style-type: none"> Detects anomalies based on real-time monitoring of user behavior, device/sim id, keystrokes patterns, etc. Minimizes DoS, transaction time, and user verification needs 	<ul style="list-style-type: none"> Proactively verifies the veracity of returns or replacement requests and alerts the business before the transaction is completed Enhances the accuracy of intent prediction and reduces false positives
Coverage of FDP approaches 	Identity proofing tools	✓	✗	✗
	Authentication tools	✗	✓	✓
	Bot mitigation	✓	✓	✗
	Device ID, telemetry	✓	✓	✗
	Behavioral biometric	✓	✓	✗
	Transaction and event monitoring	✓	✓	✓

Source: Industry reports, Secondary research, Praxis analysis

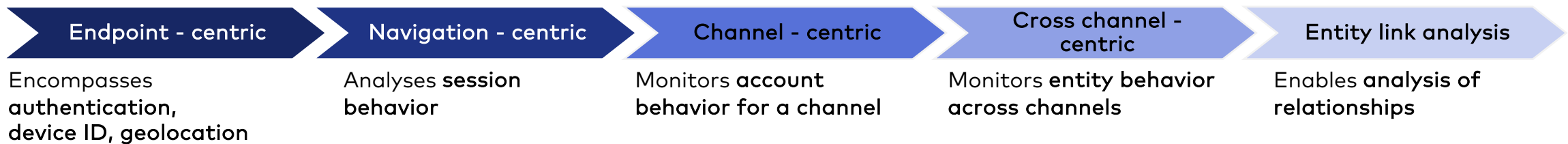
✓ Completely covered
✓ Partially covered
✗ Not covered

FDP solutions utilize various sources and techniques to acquire, analyze and report data; detection approaches can vary in sophistication based on the type of use case

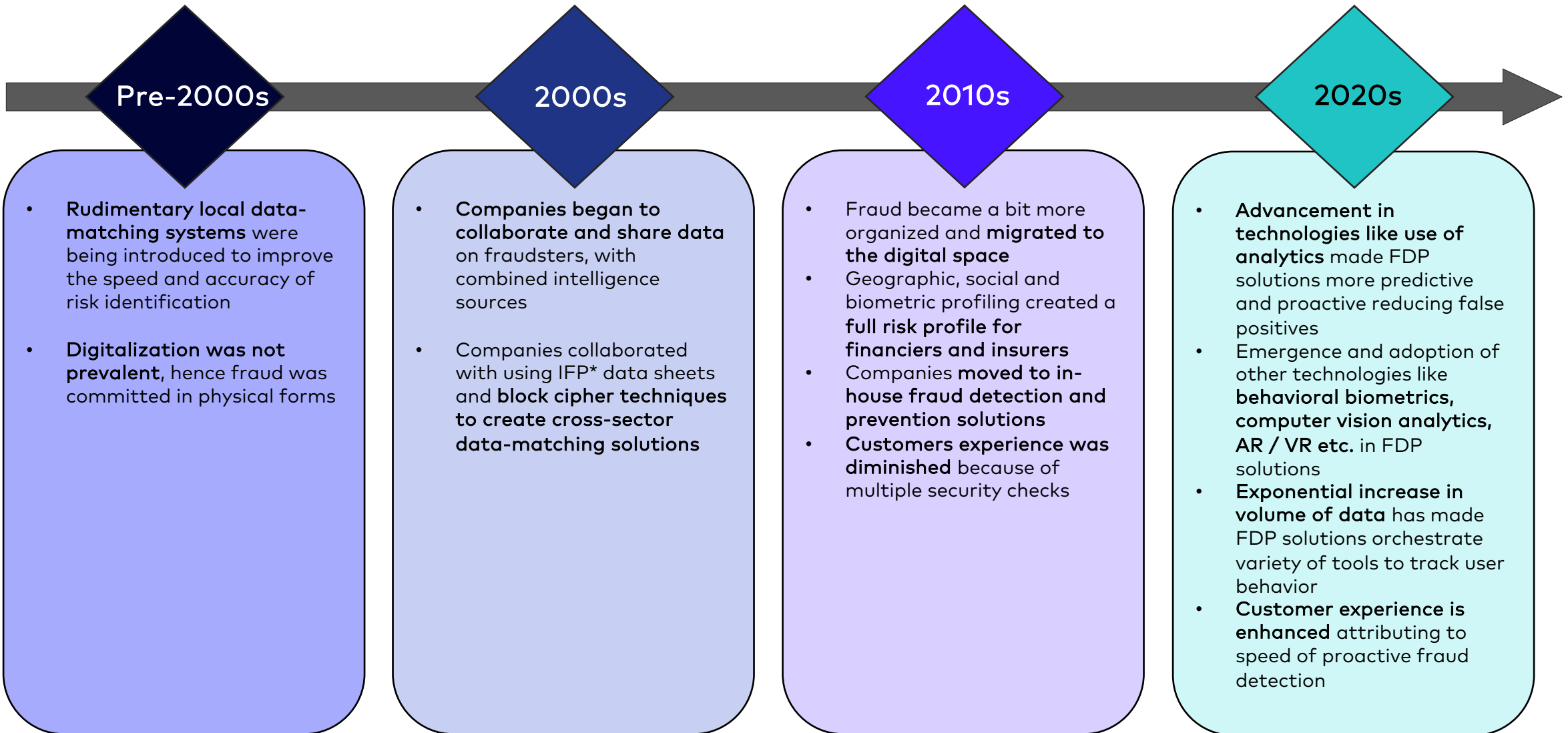
Phases of fraud detection and prevention



Levels of sophistication in fraud detection analysis



FDP solutions are becoming more sophisticated AI driven and predictive owing to advancements in AI and deep learning technologies

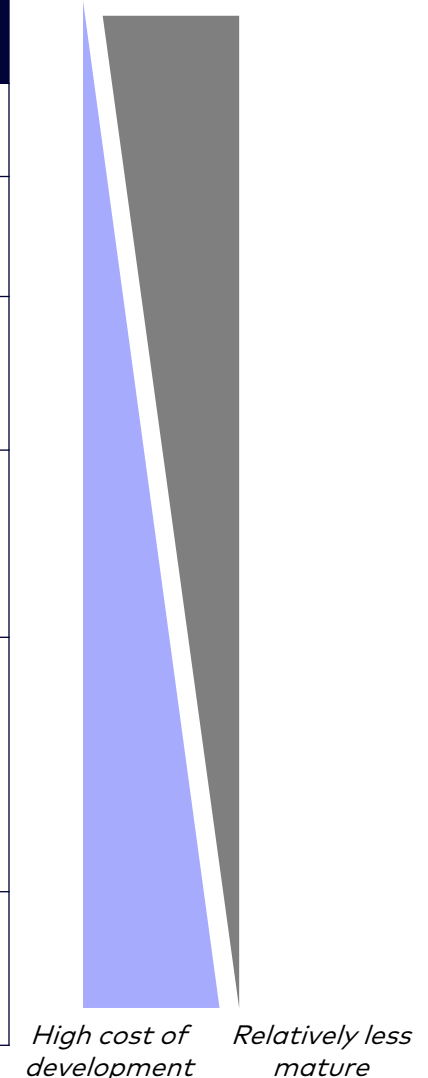


Note(s): *Intelligent Forms Processing
 Source(s): Secondary research, Praxis analysis

Physical biometrics, computer vision analytics, and behavioral biometrics are the top three utilized FDP technologies

Technology	Description	Utilized in the following phase in a digital customer journey	Examples	Expected impact on FDP tech when fully mature
Physical biometrics	<ul style="list-style-type: none"> Analyzes parameters such as - fingerprint, facial parameters or voice 	<ul style="list-style-type: none"> Account opening Login and transaction 	<ul style="list-style-type: none"> Facial scan to login to a banking app 	
Computer vision analytics	<ul style="list-style-type: none"> Use of computer or artificial intelligence for analyzing video or photographic data 	<ul style="list-style-type: none"> Account opening 	<ul style="list-style-type: none"> Liveliness tests and selfie analysis during KYC in a fintech app 	
Behavioral biometrics	<ul style="list-style-type: none"> Behavioral biometric authentication includes keystroke dynamics, gait analysis, cognitive biometrics, and signature analysis 	<ul style="list-style-type: none"> Account opening Login and transaction Post transaction 	<ul style="list-style-type: none"> Typing speed analysis to detect bot attacks 	
Data science and analytics	<ul style="list-style-type: none"> Allows a company to smartly decipher and report financial anomalies by filtering out fraudulent transactions from large datasets 	<ul style="list-style-type: none"> Login and transaction 	<ul style="list-style-type: none"> Analysis of ticket size, frequency and volume of transaction originating from a user to detect anomalies 	
Blockchain / distributed ledger technology	<ul style="list-style-type: none"> With blockchain, one can share the recorded data in real-time and update it with the approval of all parties who have access to the data but the approach needs all the participants to be on the same platform 	<ul style="list-style-type: none"> Login and transaction Post transaction 	<ul style="list-style-type: none"> Use of distributed digital id network to login to banking and logistics apps and trace authenticity of the customer and the merchant 	
Virtual / augmented reality	<ul style="list-style-type: none"> VR and AR are prime mechanisms for enabling a wider range of payment authenticators 	<ul style="list-style-type: none"> Login and transaction 	<ul style="list-style-type: none"> Usage of VR/AR technologies in rotation confuse the fraudster during the login process 	

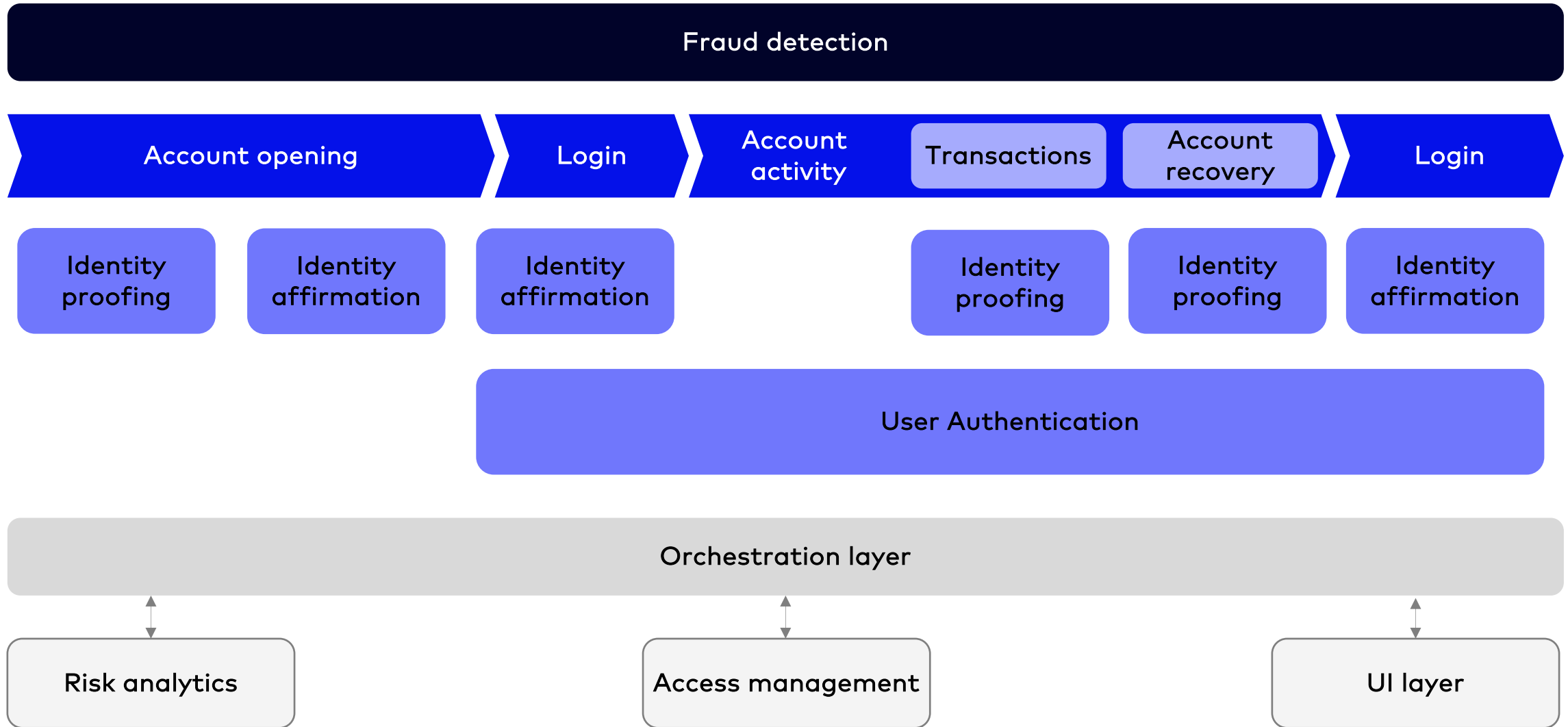
Low cost of development Most mature



Source(s): Secondary research, Praxis analysis

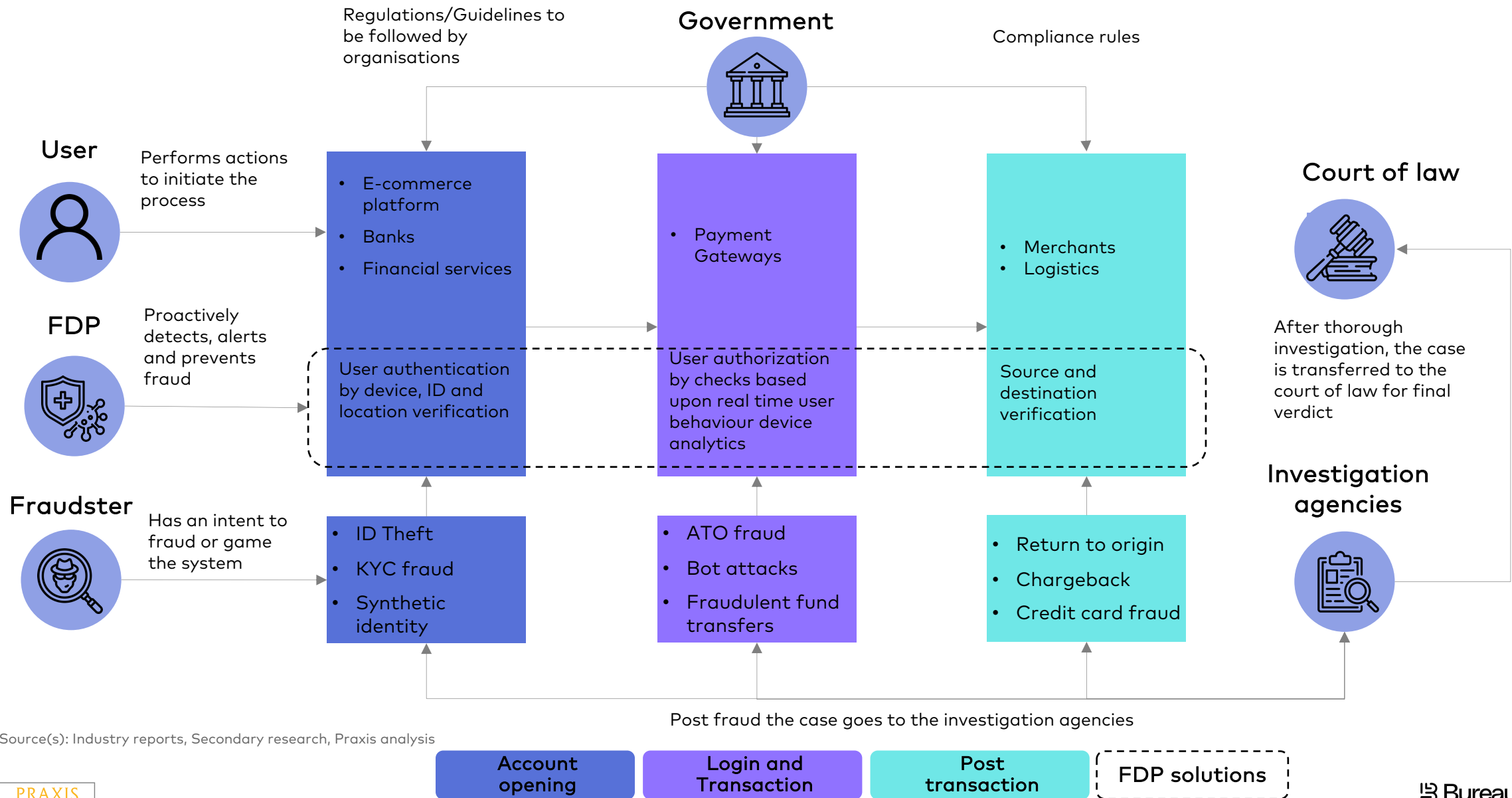


Orchestration¹ of risk management capabilities along the digital user journey



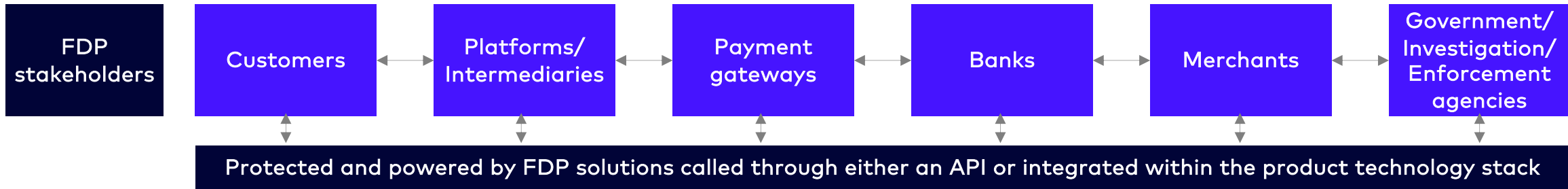
Note(s): 1. A solution that connects tools producing risk and trust signals to underlying analytics tools, and provide step-up authentication in response
Source(s): Industry reports, Praxis analysis



FDP ecosystem consists of multiple stakeholders like the user, FDP player, fraudster, Govt., Court of law and investigation agencies



Source(s): Industry reports, Secondary research, Praxis analysis

FDP solutions benefit all the participating stakeholders in an ecosystem of a digital transaction



<p>Role played by FDP solution</p> 	<ul style="list-style-type: none"> Analyzes various device and behavior metrics to alert about possible fraud 	<ul style="list-style-type: none"> Analyzes various device and behavior metrics to alert about possible fraud Continuous or event-based monitoring 	<ul style="list-style-type: none"> Continuous or event-based monitoring to detect fraudulent transactions and payment origins 	<ul style="list-style-type: none"> Continuous or event-based monitoring to detect fraudulent transactions and account origins 	<ul style="list-style-type: none"> Analyzes various device and behavior metrics to alert about possible fraud 	<ul style="list-style-type: none"> Provides extensive login and transaction related data when authorized
<p>Benefits obtained</p> 	<ul style="list-style-type: none"> Reduced customer journey time Enhanced user security and protection of consumer data Improved customer experience 	<ul style="list-style-type: none"> Enhanced customer and merchant loyalty Increased volume of purchases Increased revenue realization Minimization of loss from fraud Insurance against false positives 	<ul style="list-style-type: none"> Enhanced real time protection of fraud Reduced transaction time Increased volume of transactions Enhanced customer trust and adoption 	<ul style="list-style-type: none"> Reduced chargebacks Reduced costs of investigation Reduced internal spend on fraud talent and solutions Reactive analysis to proactive intelligence for loans and AML analysis 	<ul style="list-style-type: none"> Reduced RTOs false positives Reduced loss from fraud Repayment of cost of logistics in case of a guarantee option Improved customer experience and loyalty 	<ul style="list-style-type: none"> Better auditability of transactions More intelligence to investigate

Note(s): RTO – Return to origin
 Source(s): Secondary research, Praxis analysis

FDP solutions are wrongly assumed to be unnecessary and not worthy however, FDP solutions help enterprises in reducing fraud operational costs and false positives

Myth



FDP solutions are not worth the extra cost: The cost of implementing FDP solutions must be weighed against costs like in-house FDP technology & manpower and loss due to "false positive" alarms



External audit can effectively prevent fraud, hence no need for FDP solutions: A financial statement audit may or may not involve proactive efforts to specifically identify fraud, it is a passive detection method



FDP solutions are difficult to implement: Since FDP solutions are offered as SaaS and in most cases integrated via APIs and plug-ins, the implementation is simple and smooth



Fraud prevention is necessary only for large companies and not SMEs: Fraudsters are now targeting mostly mid-sized businesses and startups which do not have enough tech capability to combat fraud

Fact



Detects new and evolving fraud attacks: Having advanced AI / ML technology, FDP solutions enhance the chances of detecting new and unexpected fraud. Organizations have successfully witnessed a 30-50% decrease in malicious fraud with the help of FDP players



Significantly reduces chargebacks pre and post – authorization: Protects digital payments from fraud. A chargeback solution allows businesses to act on dispute inquiries and chargeback alerts in real-time post-authorization



Lowers fraud operational costs by reducing manual review rate (companies have eliminated 10 - 20K hours in manual investigations per year): **Automatically approves / declines orders** according to customizable policies, reducing the burden of manual reviews and associated operational costs



Helps to accept more good orders (reduces false positive rates by >40%) and increase revenue: Accurately assesses a customer's trustworthiness on a faster and larger scale → declining bad orders, accepting more good orders, and reducing false positives

Source(s): Industry reports, Secondary research, Praxis analysis

Budget, poor data quality and staffing limitations are the main challenges faced by FDP players; growing digitalization, high in-house FDP costs are the key drivers

Headwinds / Challenges



Budget / financial restrictions: Developing a FDP solution that is compatible for different businesses is expensive to implement



Poor data quality or integration: Integration issues arise when the quality of data from clients is not standardized



Staffing / in-house skills limitations: Staff often lack the essential skills needed to develop and implement a FDP solution



Lack of perceived ROI: Absence of expected ROI makes investments constrained



Data governance and transparency concerns: Maintaining transparency with the clients makes it challenging for FDP players to share all the data



Security risks / vulnerabilities: Clients face security risks as they share their confidential data with the FDP solution provider



Excessive false positives: Excessive false positives hamper client's reputation in front of their users

Tailwinds / Opportunities



Accelerating digitalization: Digital transformation makes businesses prone to digital fraud creating a need to deploy advanced and dynamic FDP solutions



High in-house FDP development costs: Developing an FDP solution in-house is expensive and time-consuming, hence organizations adopt FDP to **speed their time to market and improve overall CX**



Tech capabilities crunch: Developing an FDP solution requires technical capabilities and talented resources which is a challenge for most organizations



Quick installation and implementation: With the prevalence of API model, FDP solutions can be quickly implemented



Increasing advanced digital fraud: High volume of modern and more sophisticated fraud need advanced solutions that can identify the nature and origin of fraud in real time



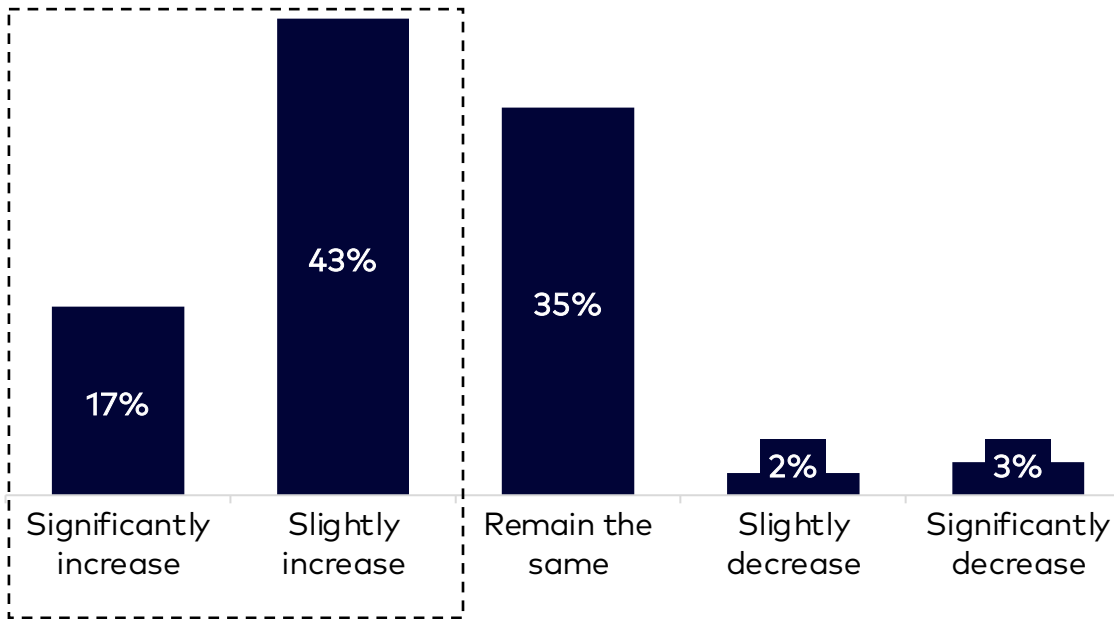
Lack of expertise: Organisations don't have the awareness and bandwidth to understand advanced digital fraud creating a need for external expert support

Organizations are expected to increase their budgets on FDP in the next two years as they look to advance their automation and analytical capabilities to fight fraud

60% of organizations are expected to increase their FDP budget

How are organizations' anti-fraud technology budgets expected to change in the next two years?

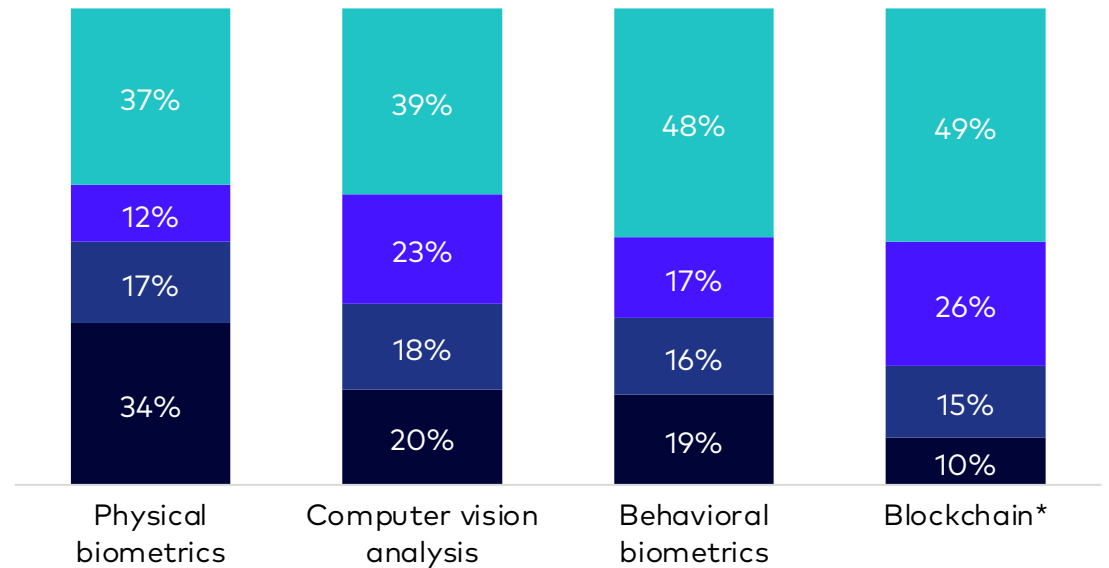
Magnitude of change in FDP budget across companies
In %, 2021



Largest spend is expected to happen on physical biometrics, followed by cognitive vision and behavioral biometrics

What emerging technologies do organizations use to fight fraud?

Spend on emerging fraud detection technologies
In %, 2021



- Currently use
- Do not currently use, but expected to deploy in more than 2 years from now
- Do not expect to use
- Do not currently use, but expected to deploy in next 1-2 yrs

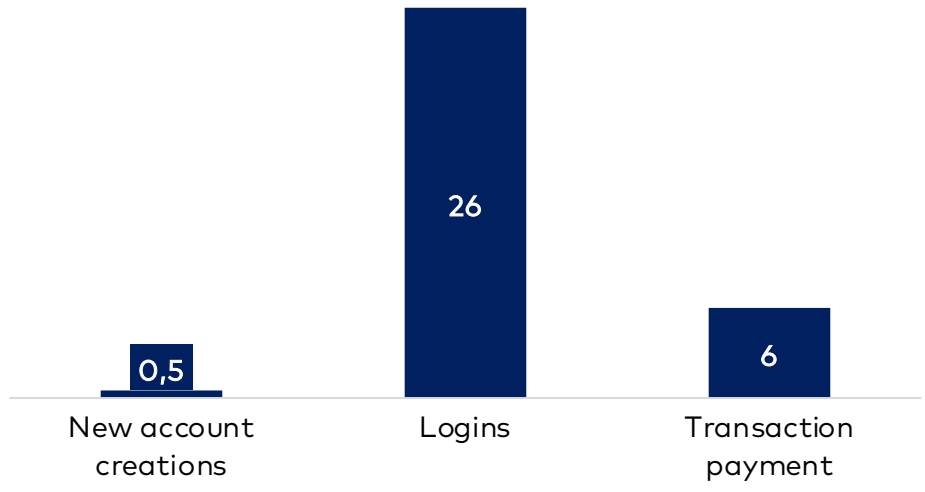
Note(s): * Distributed ledger technology
Source(s): ACFE report (survey N = 80,011) 2022, Secondary sources, Praxis analysis

Largest proportion of fraud occurs during the new account creation phase, the origin to transaction fraud; however, organizations largely monitor transactions

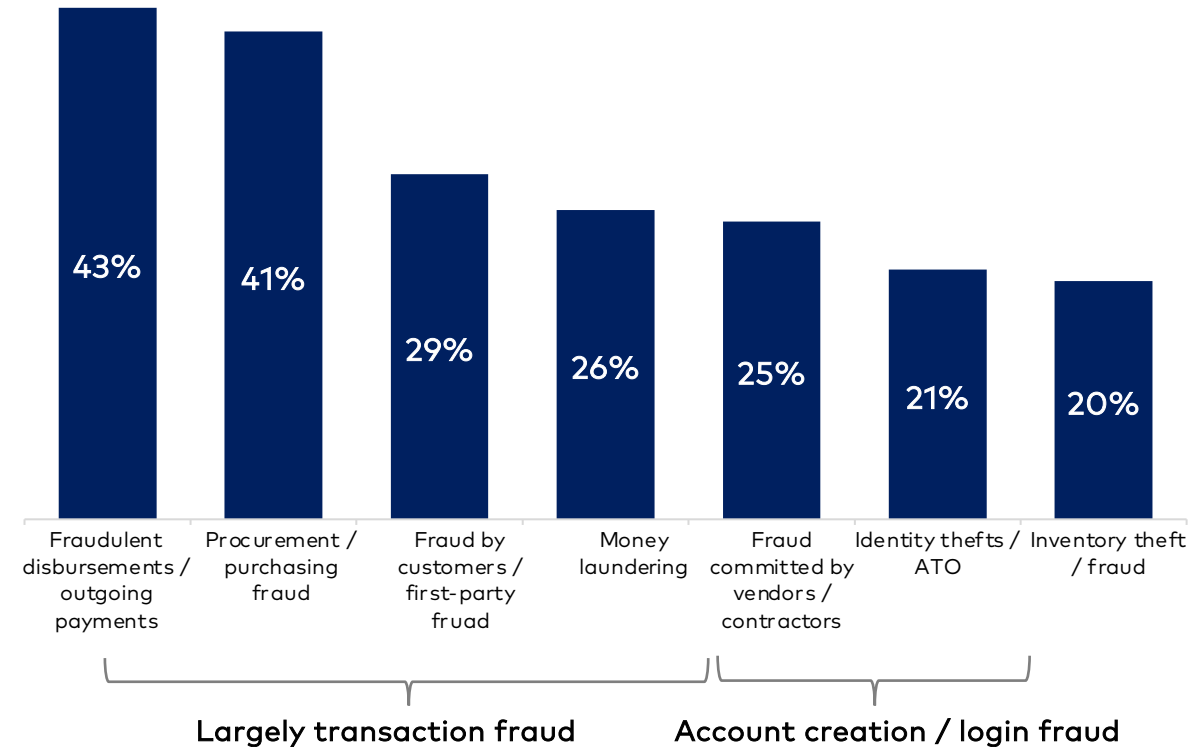
Out of the total fraud instances, 45M occurred during new account creations, 130M during logins & 192M during transaction payments

More than 26% of organizations monitor transactions

of global transactions by customer journey
In B, Jul – Dec 2021



% of companies monitoring instances of fraud
In %, 2021

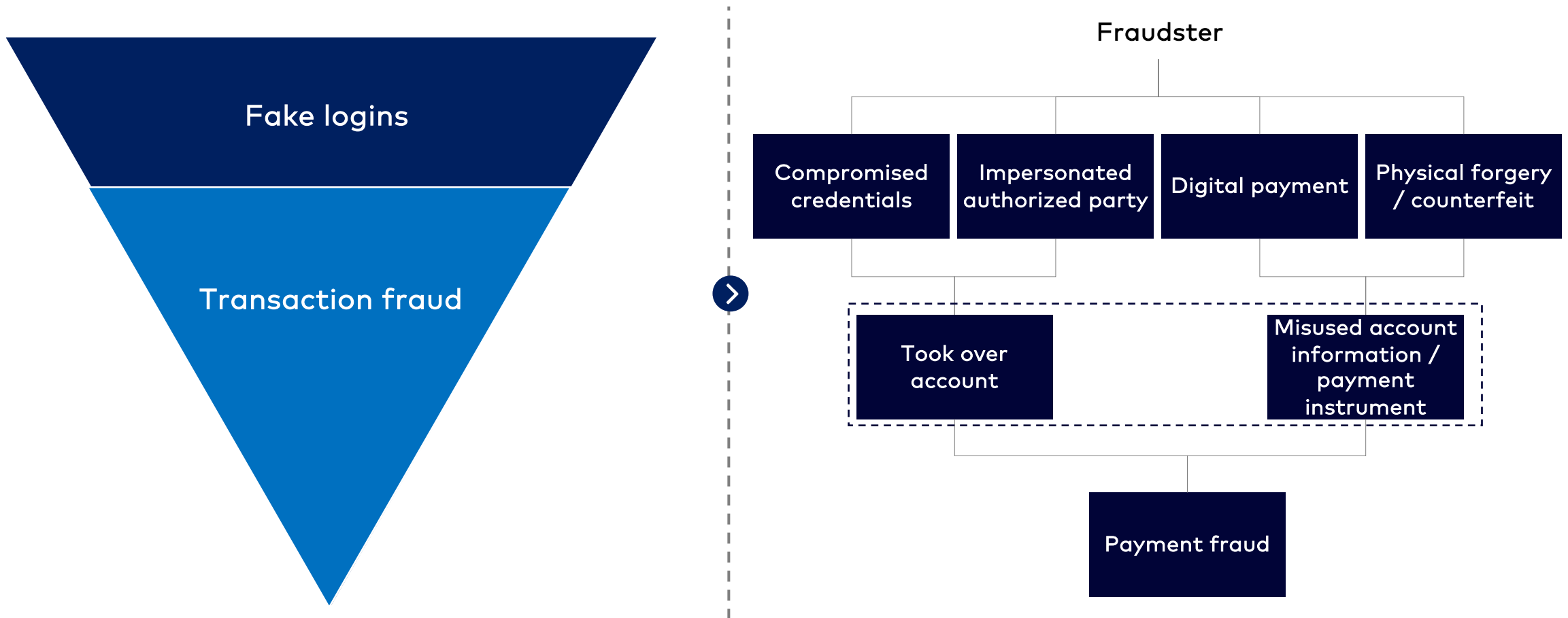


Fraudulent instances (% Jul – Dec 2021)	9.0%	0.5%	3.2%
Fraudulent instances (M, Jul – Dec 2021)	45	130	192
Fraud attack YOY (2020 -21) growth rate	50 – 70%	20 – 50%	40 – 70%

Source: Lexis Nexis report, ICEF report, Praxis Analysis

Most of the transaction fraud happens because of fake logins; FDP players and FIs should effectively monitor logins to detect fraudulent activities

Effective gate-keeping at the login stage can help in mitigating transaction-related fraud



- Bad actors once successfully onboarded in the **login stage**, it is difficult to prevent transaction fraud
- FDP players and financial institutions should have a **robust model to identify fraudulent activity at the login stage**

Source(s): Industry reports, Secondary research, Praxis analysis

Attempt to create fake logins

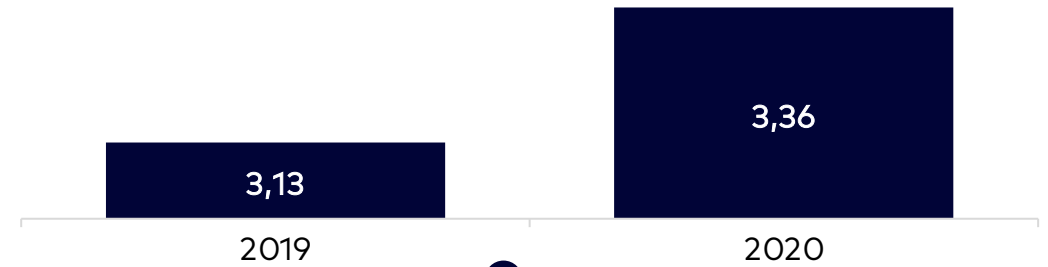
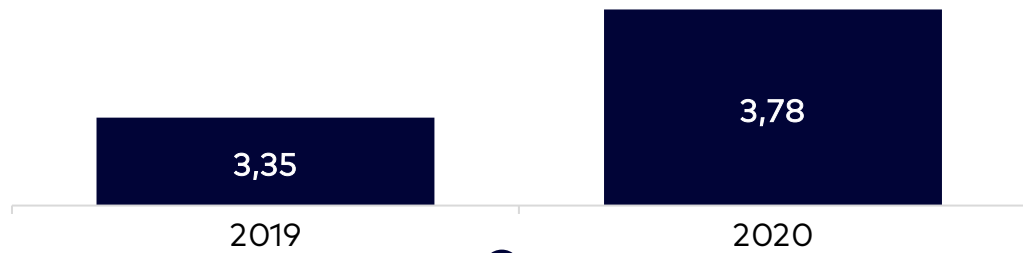
Inadequate coverage of login fraud and ineffective measures to counter fraud cost US organizations 3X - 4X of every dollar lost to fraud

Cost of fraud in FS includes fees for applying, underwriting and processing, fines, interest legal fees and cost of recovery

Cost of fraud in e-Commerce includes logistics, merchandise replacement and redistribution costs

Cost of fraud in US financial services for every US\$ 1 of fraud
In US\$

Cost of fraud in US e-commerce for every US\$ 1 of fraud
In US\$



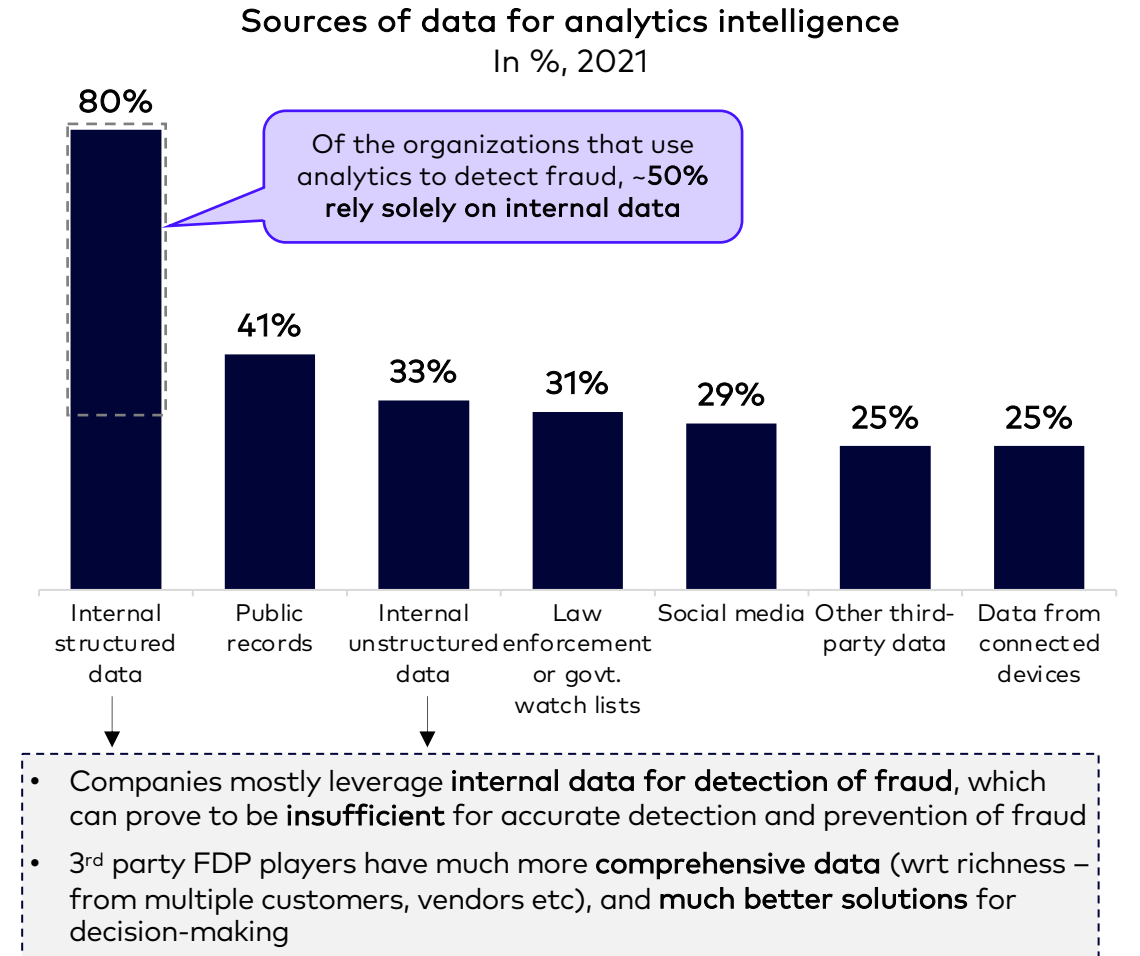
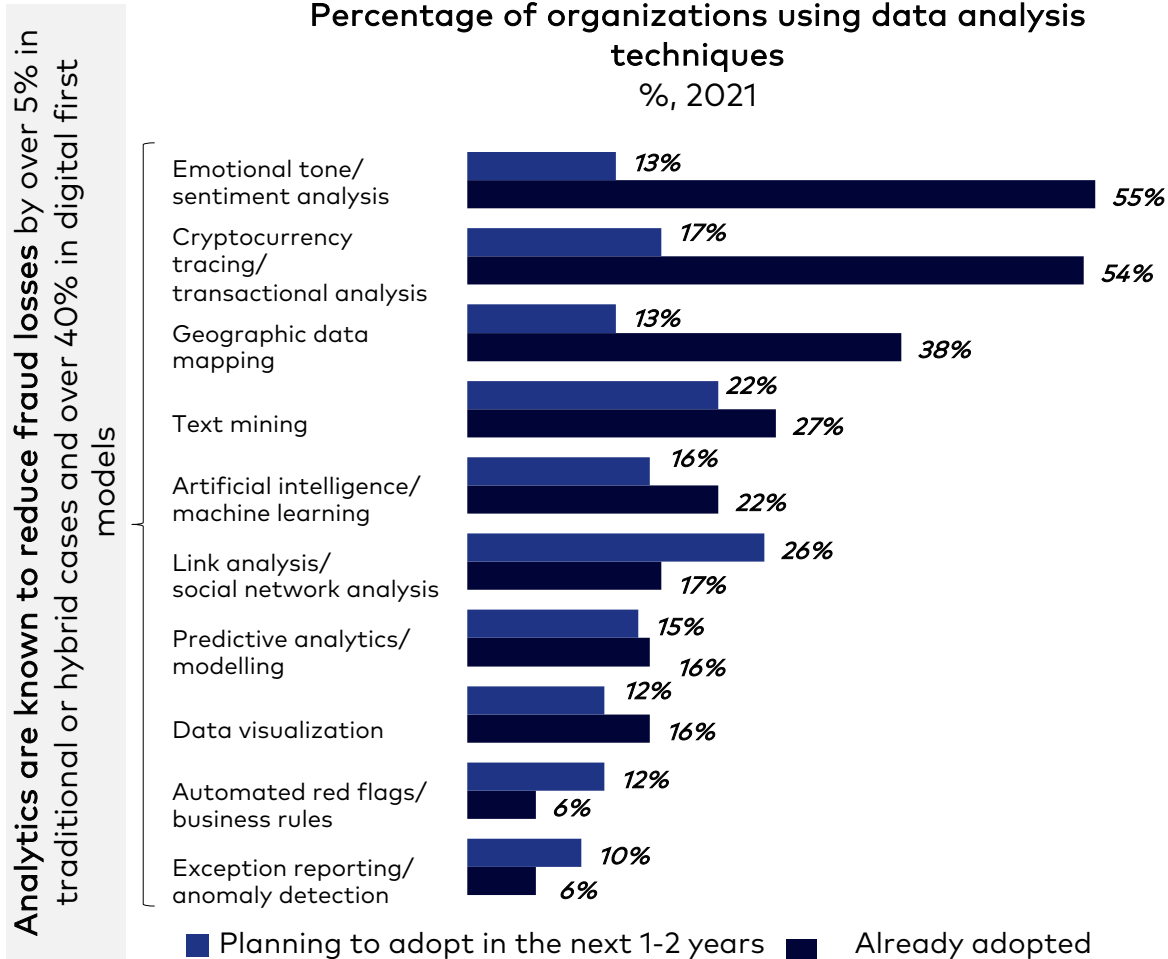
Losses	Brief description
Application fees	• Non-refundable amount charged by banks during loan application
Underwriting fees	• Collected by underwriters for securing financial instruments (stock issuances, mortgages, insurance policies)
Processing fees	• Payment processing fees are the costs that business owners incur when processing payments from customers • Processing charges - At the time of processing a loan, a bank will be bearing some cost related to administration
Fines	• Penalty on financial institutions for lacking regulatory compliance and due diligence
Interest legal fee	• Rate of interest that can be legally charged on any type of debt
Cost of recovery	• Includes investigation cost (reviewing contracts and fees)

Losses	Brief description
Logistics and redistribution cost	• Refers to the expenses of packages, transport and storage associated with each order
Merchandise replacement cost	• The amount which is spent to restock an item after it has been sold (managing inventories)

Analytics is the widest used technique to detect fraud, but its largely ineffective as organizations rely largely on internal data

~55% organizations have adopted techniques like emotional tone analysis and cryptocurrency tracing analysis to prevent fraud

Large part of the intelligence in the analytics is derived from internally structured data, resulting in weaker filtering of fraud



Source(s): ACFE report (survey N = 80,011), Secondary research, Praxis analysis

Enterprises use different deployment models to mitigate fraud

Built-in FDP



- Payment gateways and providers have their own **fraud prevention tools**
- Service gathers the **user's card and transaction data** and compares it with previous transactions



In-house FDP



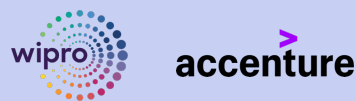
- Developing and managing **software solution and infrastructure** are **buyer's accountability**
- The **advantage** is enhanced data protection, product knowledge and integration
- **Implementation costs** are higher



Cloud based, End-to-End



- Managing software solution is the buyer's accountability while **infrastructure is outsourced to third party**
- Greater **elasticity and scalability**
- **Integration process is challenging** as it involves extra integration costs, additional support fees and multi-year contracts



API based solutions



- A **fraud prevention API** meets the needs of modern, cloud and web-app powered businesses
- API calls are **fast, affordable** and becomes useful in case of tech stack
- Several APIs exist across the ecosystem; **one license per provider** is needed which aggravates the costs



Multi-layered approach



- When more than one solution is needed then organizations go for **multi-layered solutions**
- Multi-layered solutions are used to **enrich the data, to meet scalability** issues, to **patch holes** in the line of defense and to **speed up manual reviews**



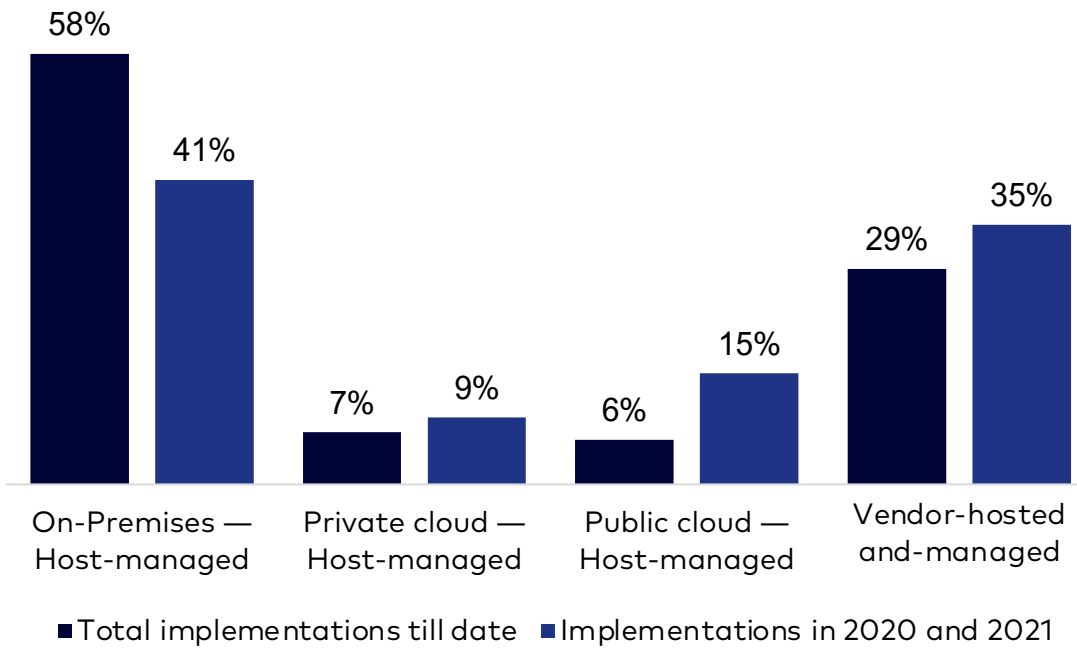
Source(s): Seon report, Secondary research Praxis analysis







Although the large proportion of FDP solutions are developed on-premise, there is an increasing trend towards adopting SaaS technologies

Industries are shifting towards cloud based deployment models for transaction monitoring in the recent years

Inefficient FDP techniques, budget constraints and talent crunch are the main drivers for adoption of FDP SaaS solutions

Implementations of transaction monitoring solutions deployments in industries
% of client deployments

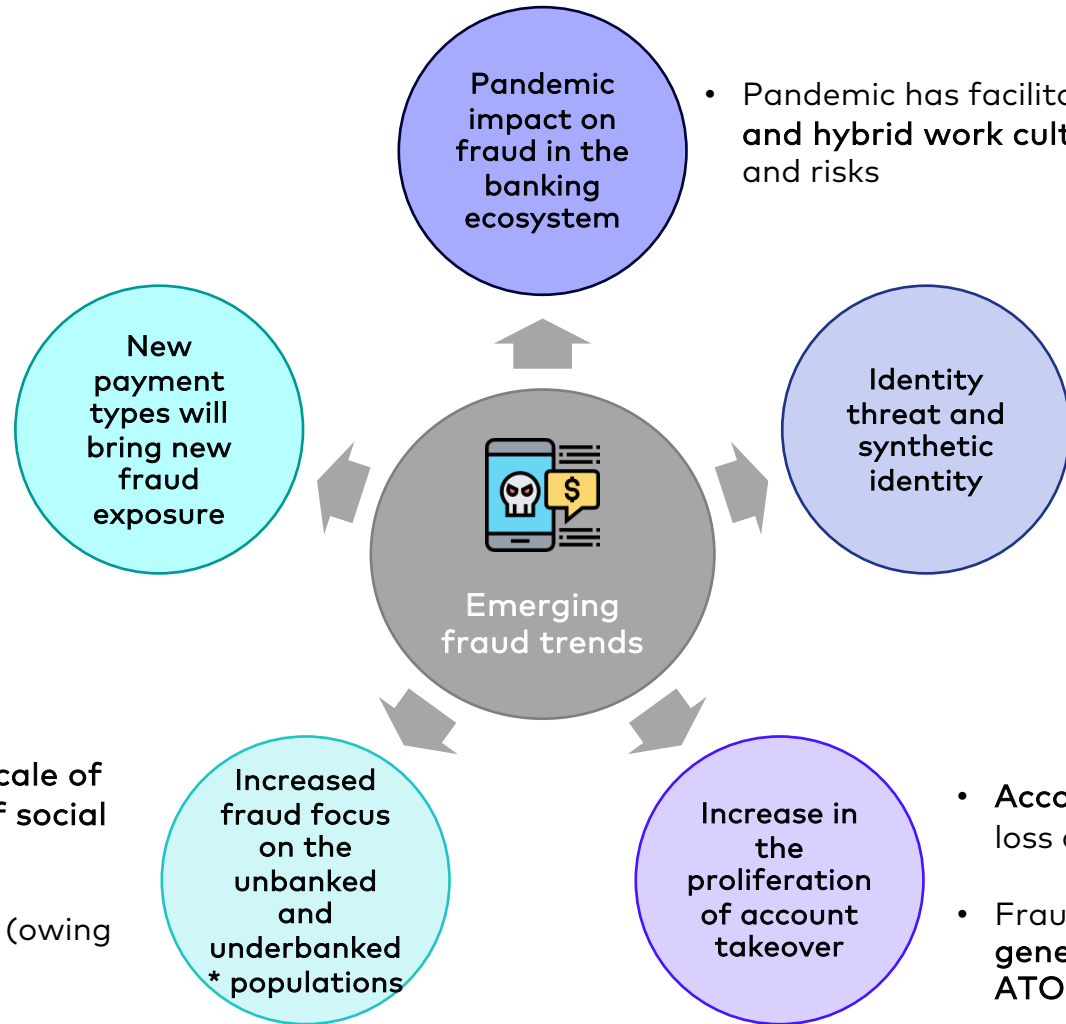


 <p>Inefficient FDP techniques adopted</p>	<ul style="list-style-type: none"> Current FDP techniques adopted fail to mitigate advanced fraud creating a need to adopt advanced AI and ML driven FDP solutions
 <p>Budget constraints</p>	<ul style="list-style-type: none"> Development of in-house FDP solution requires technology and workforce incurring higher costs
 <p>Talent and technology crunch</p>	<ul style="list-style-type: none"> Organizations lack talented pool of resources and technologies required to develop FDP solutions
 <p>Limited exposure to different type fraud</p>	<ul style="list-style-type: none"> SaaS FDP solutions have significantly better exposure to varied use cases of fraud making them well equipped to prevent varied fraud
 <p>Excessive false positives</p>	<ul style="list-style-type: none"> Excessive false positives make it challenging to identify and mitigate fraud which is reduced with the adoption of advanced FDP solutions
 <p>Pricing models</p>	<ul style="list-style-type: none"> The pricing offered by SaaS FDP solutions providers is flexible and relatively lower

Source(s); Gartner report (Survey of clients N = 1,150), Secondary research, Praxis analysis

Pandemic coupled with automated payments facilities and banking initiatives have accelerated risk of fraud globally

- **New automated payment types** (like invisible payments, etc.) provide challenges to banks in widening the **omnichannel monitoring requirement**
- Fraudsters are highly likely to attempt to exploit these **nascent payment methods** and the **changing payment authorization paradigm**



- Pandemic has facilitated **new digital offerings and hybrid work culture** → increase in threats and risks

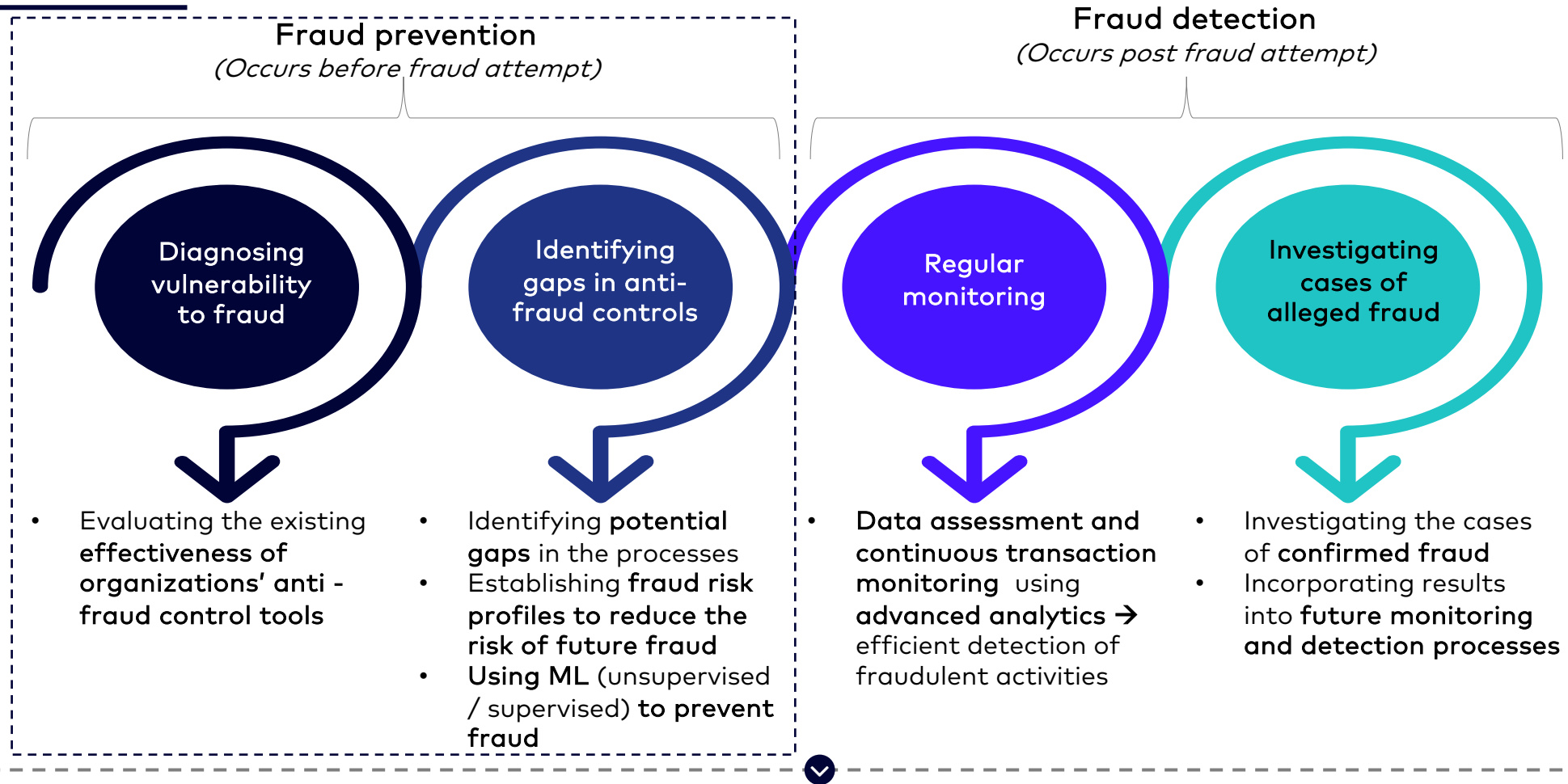
- **Data breaches** will occur at an increased scale → **increase of identity fraud and account takeover fraud**
- **85%+ of the synthetic identities** are missed by traditional fraud models per ID Analytics research

- **Increase in frequency and scale of scams and sophistication of social engineering techniques**
- **Target unbanked consumers** (owing to their very limited banking knowledge)

- **Account Takeover (ATO)** is a significant loss area in most global markets
- Fraudsters are expected to shift focus from **generalized attacks to more-targeted ATO attacks**

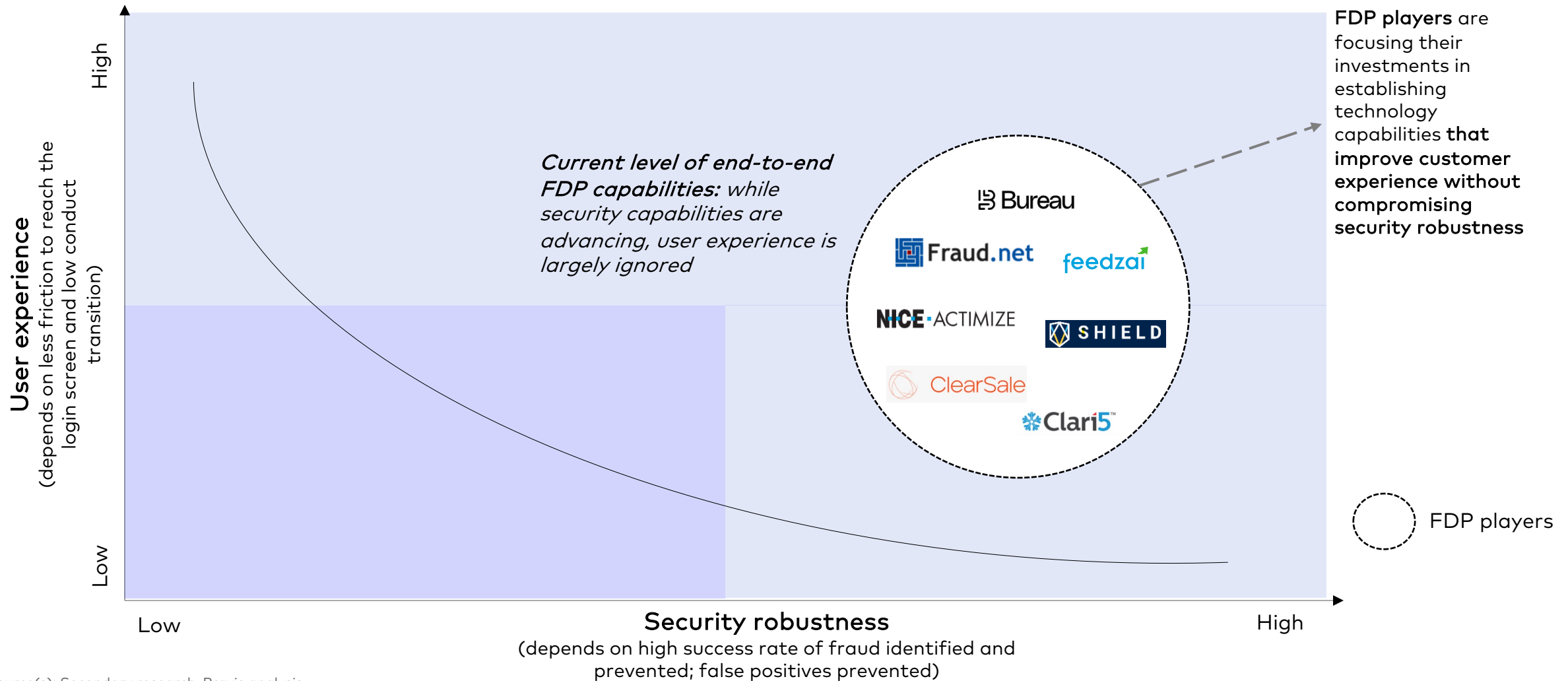
Note(s): Unbanked and underbanked* population are those who don't have bank account and / or need to rely on alternative financial services outside of the banking system; Invisible payment** where the payment is triggered automatically, via location or action, without the consumer having to do anything
 Source(s): White paper by riskCanvas, Secondary research, Praxis analysis

With real-time monitoring and ML techniques, FDP SaaS players prevent fraudulent activities before they occur



- New-age SaaS FDP players help organizations not only in detecting fraud post occurrence but also in preventing fraud from occurring by using advanced analytics → reduced losses
- Fraud prevention is important as it helps in reducing financial loss, improving customer loyalty, increasing customer retention, and preventing the impact of fraud on organization morale

FDP buyers need solutions that can balance user experience with robustness of fraud prevention



Source(s): Secondary research, Praxis analysis

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

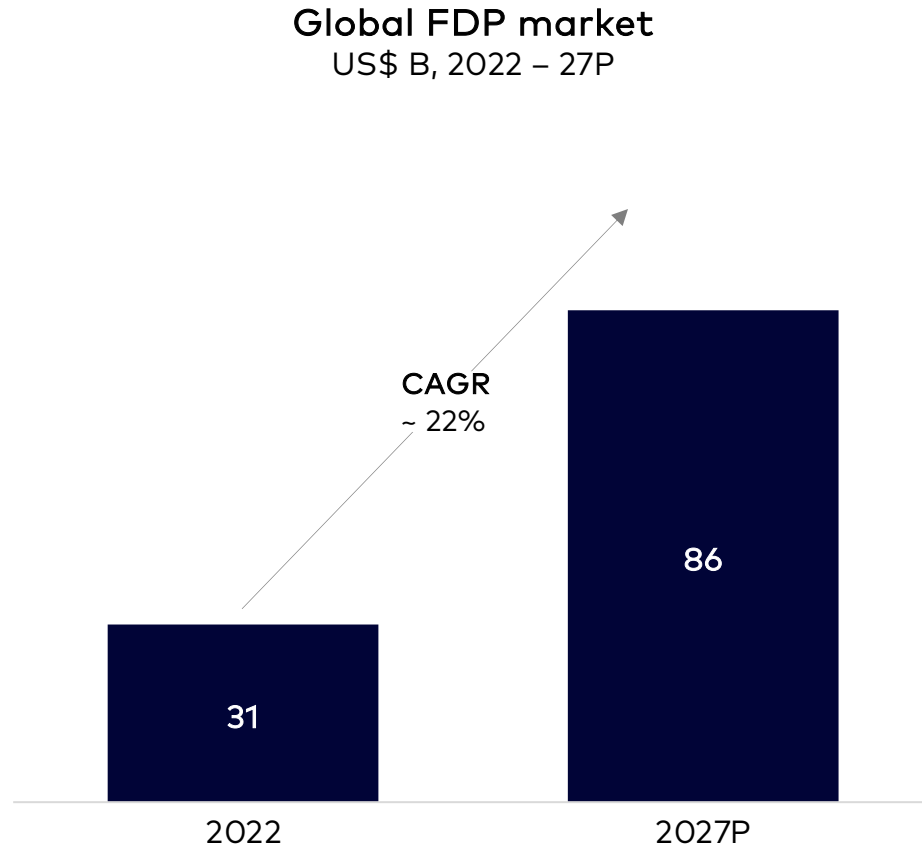
FDP market landscape in Southeast Asia

FDP playbook





Appendix

The global FDP market stood at ~US\$ 31B in 2022, growing at ~22% CAGR and is expected to reach ~US\$ 86B in 2027

The global FDP market is projected to be ~US\$ 86B in 2027, growing at a CAGR of 22%



Growing adoption of online applications, digital payments, digitization and IoT have propelled the global FDP market growth

Growth factor	Details
 Increasing online applications & mobile banking	<ul style="list-style-type: none"> Global internet users increased by 6.4% annually 2018-21 Growing adoption of online applications and mobile banking services → many fake websites and mobile applications
 Adoption of digital payments and NFC technology	<ul style="list-style-type: none"> A large population has shifted to online transactions (~40% adults use e-commerce, ~66% adults conduct online financial transactions) As card-chip technology matures and new digital channels emerge, increasing number of points of vulnerability are exposed
 Adoption of digitization and IoT	<ul style="list-style-type: none"> Connected devices collect, transmit, and store various consumer data, which creates privacy risks and presents easier access for fraud
 Emergence of big data analytics	<ul style="list-style-type: none"> Big data uses advanced analytics techniques such as machine learning, predictive analytics to analyze data sets

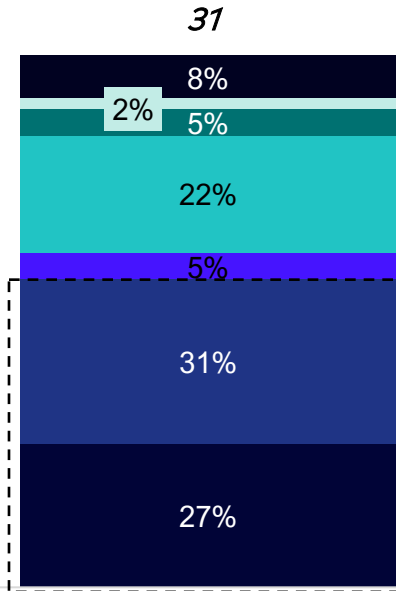
Source(s): Industry reports, Secondary research, Praxis analysis

Banking and FS constitute ~60% of current FDP market; North America will continue to dominate the FDP market till 2027 while APAC will be the fastest growing region

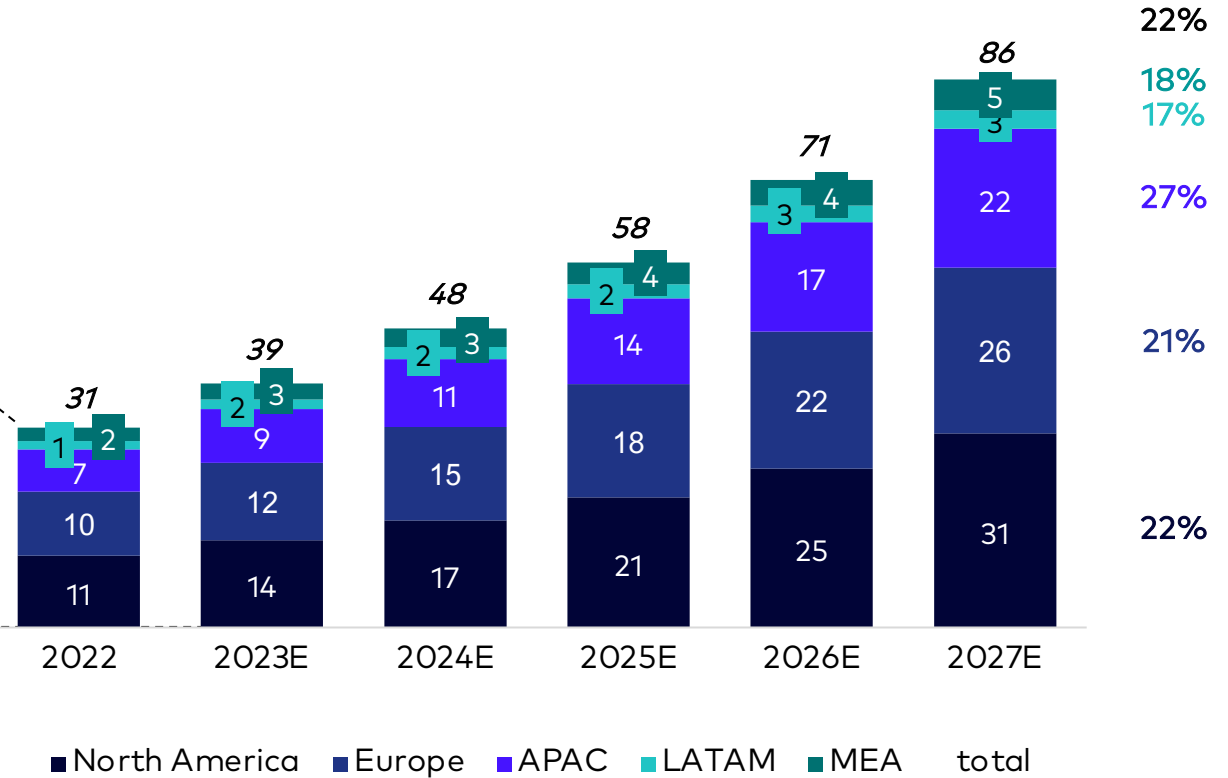
E-Commerce constituted 22% of FDP market in 2022, 3rd largest after banking and financial services

Catalyzed by the increasing digitization and GDP per capita, APAC is expected to maintain the highest growth rate till 2027

FDP market by verticals
In US\$ B, 2022



FDP market by geographies
In US\$ B, 2022 – 27P

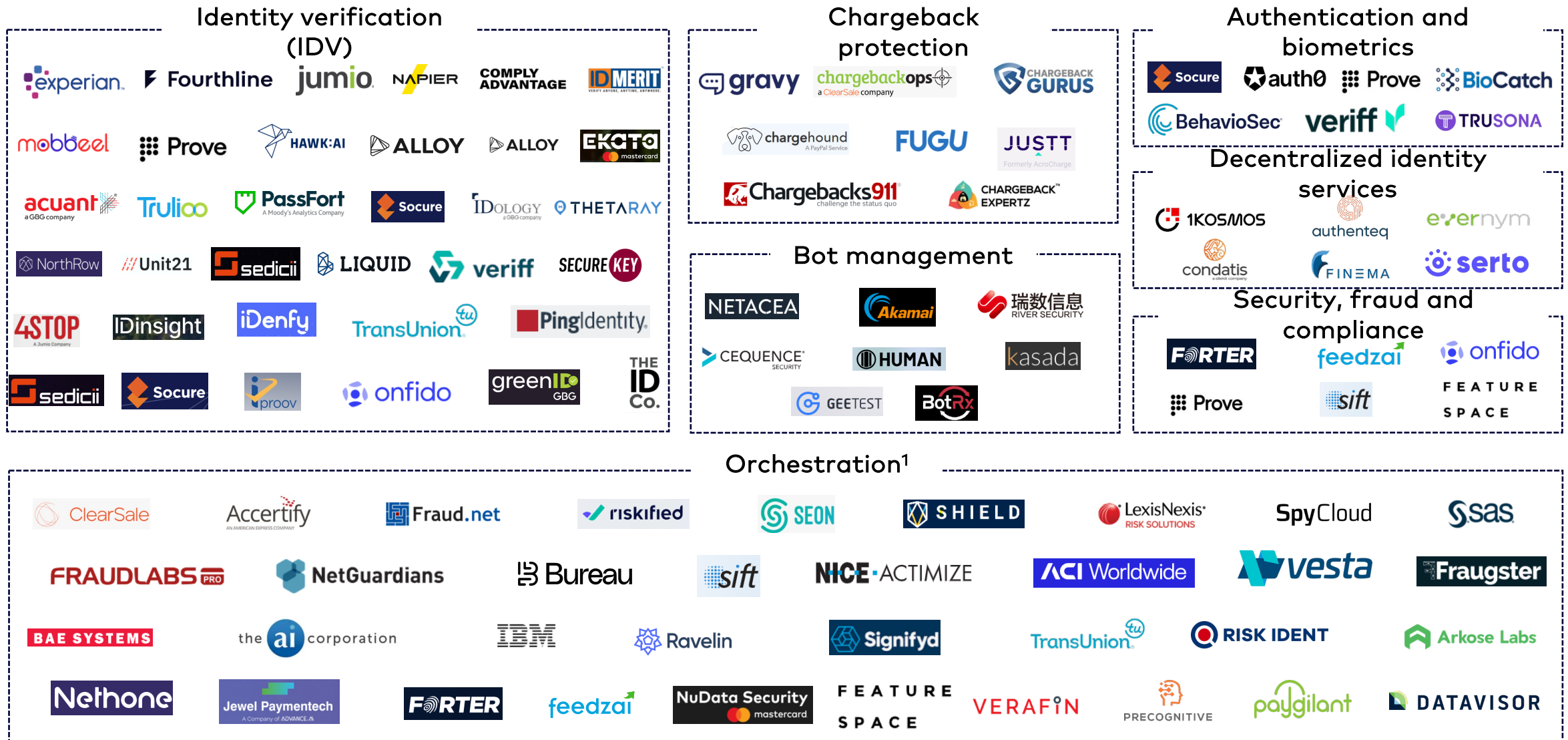


- Banking
- E-commerce
- Others
- Financial services
- Real money gaming
- Insurance
- Gig economy

- North America
- Europe
- APAC
- LATAM
- MEA
- total

Source(s): Secondary research, Praxis analysis

Global FDP landscape is evolving rapidly



Note(s): 1. A solution that connects tools producing risk and trust signals to underlying analytics tools, and provide step-up authentication in response; This is not an exhaustive list of FDP players

Source(s): Industry reports, Company websites, Praxis analysis

Governments of US and UK have passed key regulations which in turn will promote the adoption of FDP solutions amongst enterprises



TCPA, CCPA, authentication guidance and KYC mandate are the major regulations passed by the US govt











Strong customer authentication, PSD2, GDPR are the major fraud prevention regulations in UK







Regulations	Brief description
Telephone Consumer Protection Act (TCPA)	<ul style="list-style-type: none"> The TCPA is a federal statute designed to safeguard consumer privacy by restricting telemarketing communications
California Consumer Privacy Act (CCPA)	<ul style="list-style-type: none"> The CCPA is a state-wide data privacy law that regulates how businesses all over the world are allowed to handle the personal information of California residents
Authentication guidance	<ul style="list-style-type: none"> Encourages FIs to use enhanced authentication controls, like multi-factor authentication (MFA) as single-factor authentication often results in unauthorized access
KYC regulations	<ul style="list-style-type: none"> Identity verification is a critical component of KYC regulations Emphasize digital identity verification methods such as ID document verification and facial comparison

Regulations	Brief description
Strong Customer Authentication (SCA)	<ul style="list-style-type: none"> Intended to enhance the security of payments and limit fraud during the authentication process Companies must provide several different methods of authentication for customers
Second Payment Services Directive (PSD2)	<ul style="list-style-type: none"> Regulation for electronic payment services Intended to make payments more secure, boost innovation and help banking services adapt to new technologies
General Data Protection Regulation (GDPR)	<ul style="list-style-type: none"> It is a law that sets guidelines for the collection and processing of personal information from individuals
UK digital identity and attributes trust framework	<ul style="list-style-type: none"> This enables people use and reuse their digital identities and will unlock improved user experience in the digital world

Successful FDP SaaS players have advanced machine learning capabilities and deep data integrations

Success factors	Brief description
 Advanced analytics and reporting	<ul style="list-style-type: none"> • Using AI / ML to adapt risk management rules to avoid false positives and decrease "customer insult" rates • Proactively predicting a fraudulent behavior by analyzing and profiling physical and behavioral metrics on device <ul style="list-style-type: none"> – Hand positions, geolocations, speed of typing etc. in conjunction with automated document verification and manual approvals for KYCs • Ability to provide clear reports
 Multi-layered solution approach	<ul style="list-style-type: none"> • Customized to each phase of the customer journey and transaction channel • Each stage of the customer journey is regarded as a unique interaction, requiring different types of identity verification, data, and solutions to prevent fraud
 Seamless customer experience	<ul style="list-style-type: none"> • Poorly designed authentication experiences have a disproportionate impact on customer engagement, fraud mitigation, and operational efficiency • Reducing the number of clicks or screen changes to login or conduct a transaction while sustaining or increasing robustness of security ensures greater adoption of the FDP solution
 Real-time monitoring	<ul style="list-style-type: none"> • Execution of fraud detection algorithms in microseconds instead of relying on databases that give historical identity or transactional data
 Flexible decisioning	<ul style="list-style-type: none"> • Customized models are leveraged based on the phase in customer journey, use case and data, that dynamically alter <ul style="list-style-type: none"> – Fraud detection rules – Data fields for analytics – Thresholds for automatically approving or rejecting an action – Targeting different touchpoints such as login, signup or withdrawals
 Ease of integration	<ul style="list-style-type: none"> • Easy integration in the minimum possible time with a clear understanding of how the FDP tool will integrate with the platform • Providing support and training for smooth integration
 Digital footprint	<ul style="list-style-type: none"> • Ensure that FDP solution can scan several social media networks, shopping behavior, OTT platforms to get a 360-degree view of users
 Efficient partnership	<ul style="list-style-type: none"> • Good network of partners (bureaus, government, channel partners, etc.) to source data that leads to better accuracy of fraud detection

FDP solutions provide seamless CX, access to large datasets, orchestration capabilities etc. and hence help in overcoming white spaces across verticals

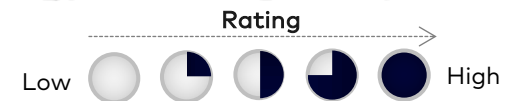
	Key needs	White spaces across verticals
	Seamless customer experience	<ul style="list-style-type: none"> Manual verification of identity proofs is both time consuming and error prone Multiple checks diminishes UX Multi-factor authentication can be a cumbersome process
	Access to large dataset	<ul style="list-style-type: none"> Companies across verticals have access to very limited data and hence, they depend on static approaches (i.e. depends only on historic data) → inaccurate fraud detection
	Orchestration capabilities	<ul style="list-style-type: none"> Lack of end-to-end solutions for monitoring fraud across the digital customer journey Certain industries like banking, insurance, etc. have disparate teams for fraud detection and prevention → latency
	Advanced fraud detection	<ul style="list-style-type: none"> Weak transaction monitoring system Weak identity verification process Static approaches (depends only on historic data) → low accuracy High false positive rate
	Real time transaction monitoring	<ul style="list-style-type: none"> Lack advanced techniques to provide real time monitoring → longer response time and increased fraud losses Most companies follow post-facto monitoring process
	Compliant with government regulations	<ul style="list-style-type: none"> Govt is gradually increasing focus towards fraud detection and has laid down various regulations like 2-factor authentication, KYC process, etc.

How can FDP players help?

- FDP solutions reduce the need for manual checks, multiple user touchpoints → **frictionless authentication and enhanced customers**
- Strong API for sourcing large databases** from multiple channels (like bureaus, aggregators, telcos)
- Gather and analyze **large volumes of clientele data** within and across industries
- FDP solutions have **great orchestration capabilities** i.e. they provide **end-to-end** complete solutions to the clients
- AI / ML expertise** to detect and prevent fraud across customer journey
- Real-time monitoring, behavioral biometrics, device metrics, keystroke dynamics, predictive analytics** are key techniques used by FDP players to ensure robust security
- Execution of fraud detection algorithms** in microseconds with the help of **advanced analytics**
- FDP solutions provide stringent checks for fraud monitoring, **complying with all govt regulations**; and are rapidly evolving with the industry and govt standards

The key purchase criteria for a FDP solution are the strength and customizability of its rule engine, pricing model, and ease of integration

Most important	Purchase criteria	Sub criteria	Customer rating	
	Features	<ul style="list-style-type: none"> • Fraud detection accuracy and false positive rate • Machine learning and adaptive capability of the rule engine • Shortest response time • Customizability/configurability • Chargeback guarantee • End-to-end solutions or orchestration capability 		<p>"Single tap logins without any password / OTP but with great security is one of the most required features for us to ensure seamless customer experience"</p> <p><i>- Fraud prevention manager, Fintech</i></p>
	Cost	<ul style="list-style-type: none"> • Pricing model <ul style="list-style-type: none"> - Deployment cost - Monthly fees or subscription model - Micro fees based on API calls • Free trial and proof of concept 		<p>"Seamless integration of FDP solution with our traditional software in the shortest possible time, without much changes to our existing system and with proper guidelines and training toolkit is quite important for us"</p> <p><i>- Product manager, BFSI</i></p>
	User experience	<ul style="list-style-type: none"> • Frictionless UX – seamless onboarding, frictionless authentication • Ease of usage – search function, logging function, flexible data representation • Ease of maintenance • Ability to streamline operations 		<p>"Our current FDP platform is commonly used amongst companies in BFSI industry and also has great reviews about the accuracy of fraud detection and ease of integration, hence we thought of going ahead with this FDP player"</p> <p><i>- Fraud prevention manager, BFSI</i></p>
	Integration and support	<ul style="list-style-type: none"> • Ease of integration of the FDP platform with existing tech tools • Support and training for smooth integration 		
	Vendor reputation	<ul style="list-style-type: none"> • Reliability and credibility • Post-sale support • Reputation & customer reviews • Recommendation from peers 		



Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

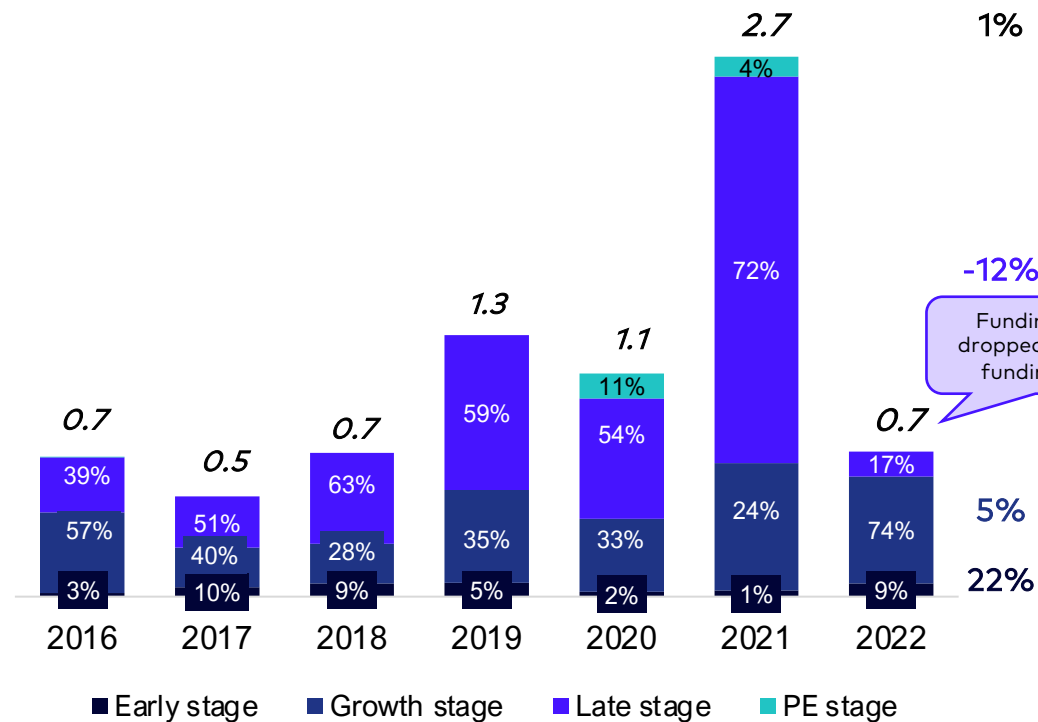
Funding in FDP players dropped significantly in 2022, due to the funding winter globally; plethora of strategic acquisitions happened in FDP space

FDP players raised ~US\$ 0.7B funding in 2022; 70%+ companies have raised funding in growth stage in 2022

Large global FDP players acquire firms to expand their geographical footprints and augment their capabilities

Investment influx in FDP players
US\$ B, 2016 - 22

CAGR
2016 - 22



1%

5%

22%

Deal count (in #)	2016	2017	2018	2019	2020	2021	2022
	77	77	80	89	78	79	55

Acquirer	Target	Acq. year	Acq. price (US\$ M)	Rationale
TransUnion	Verisk	2023	2.7	<ul style="list-style-type: none"> To expand its portfolio to AML and eliminate the need for separate searches across different AML databases and different watch lists
SEON	complytron	2022	515	<ul style="list-style-type: none"> To provide customers with better market insight and fraud prevention services It will work on integrating Verisk's services them into the Prama analytics platform
EQUIFAX	MiDiGATOR	2022	-	<ul style="list-style-type: none"> To expand its global footprint in digital identity and fraud prevention Midigator's highly automated, data-driven chargeback prevention and management solutions along with Kount's AI solution will supplement to Equifax's bureau capabilities
	Kount	2021	640	
GBG	acuant	2021	736	<ul style="list-style-type: none"> To augment its capabilities To strengthen its offering in Europe and APAC To expand into the US market

Source(s): Secondary research, Praxis analysis

Budget, poor data quality and staffing limitations are the main challenges faced by FDP players; digitalization and growth in fraud are the major demand drivers

Headwinds / Challenges



Budget / financial restrictions: Developing a FDP solution that is compatible for different businesses is expensive to implement



Poor data quality or integration: Integration issues arise when the quality of data from clients is not standardized



Staffing / in-house skills limitations: Staff often lack the essential skills needed to develop and implement a FDP solution



Lack of perceived ROI: Absence of expected ROI makes investments constrained



Data governance and transparency concerns: Maintaining transparency with the clients makes it challenging for FDP players to share all the data



Security risks / vulnerabilities: Clients face security risks as they share their confidential data with the FDP solution provider



Excessive false positives: Excessive false positives hamper client's reputation in front of their users

Tailwinds / Opportunities



Accelerating digitalization: Digital transformation makes businesses prone to digital fraud creating a need to deploy advanced and dynamic FDP solutions



High in-house FDP development costs: Developing an FDP solution in-house is expensive and time-consuming, hence organizations adopt FDP to **speed their time to market and improve overall CX**



Tech capabilities crunch: Developing an FDP solution requires technical capabilities and talented resources which is a challenge for most organizations



Quick installation and implementation: With the prevalence of API model, FDP solutions can be quickly implemented



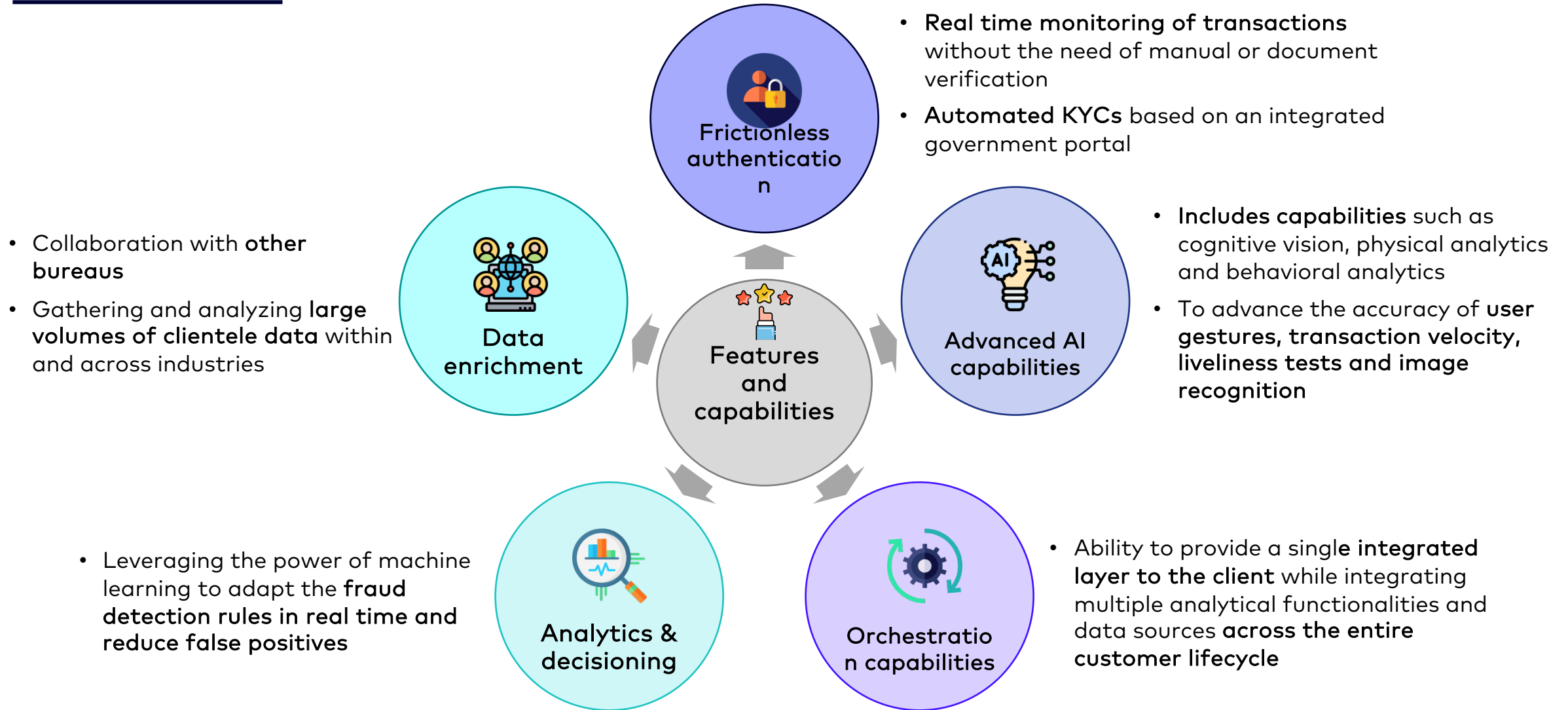
Increasing advanced digital fraud: High volume of modern and more sophisticated fraud need advanced solutions that can identify the nature and origin of fraud in real time



Lack of expertise: Organisations don't have the awareness and bandwidth to understand advanced digital fraud creating a need for external expert support

Source(s): Industry reports, Secondary research, Praxis analysis

FDP SaaS players should invest in following capabilities to enhance their competitive and price advantage in the next 3-5 years



Source(s): Industry reports, Secondary research, Praxis analysis

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

FDP market landscape in Southeast Asia

FDP playbook

Appendix

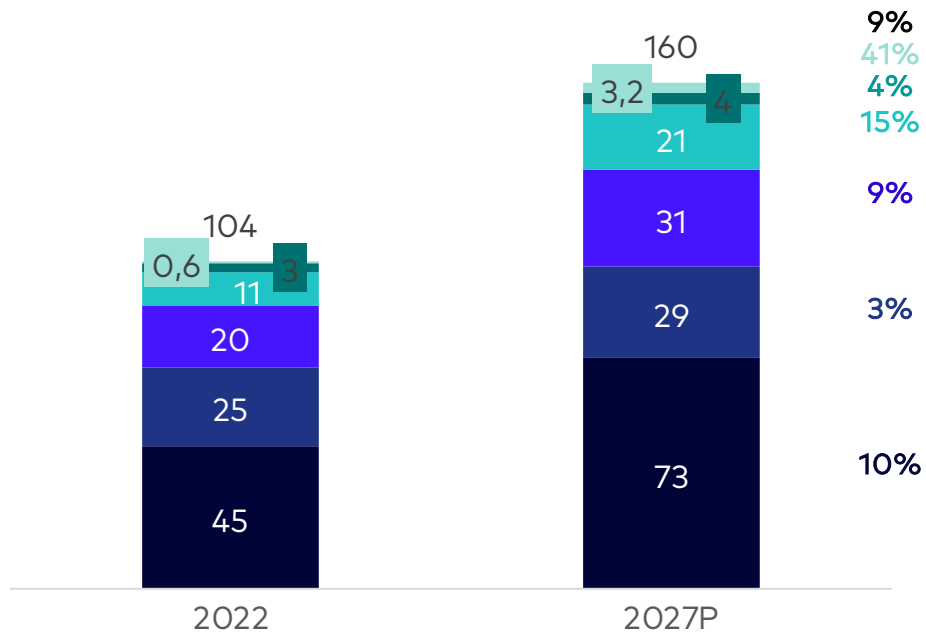
Indian enterprises are increasing spending on IT, ~US\$ 104 B was the spend on IT in 2022, with software emerging as the highest growing segment

IT spending in India is estimated at US\$ 104 B in 2022, and is expected to reach US\$ 160 B in 2027

Growing number of digital-first businesses and policies favoring digital India are driving IT spending in India

India's IT spending
In US\$ B, 2022 – 27P

CAGR
2022 –
27P









9%
41%
4%
15%

9%
3%

10%

- Devices
- IT Services
- Data Center Systems
- Communication Services
- Software
- FDP

Source(s): Gartner, Secondary research, Praxis analysis

 <p>Growing number of digital-first businesses</p>	<ul style="list-style-type: none"> • 2x growth in micro businesses actively transacting online • ~75% mom & pop stores in metros are working towards going online
 <p>Rising technology adoption</p>	<ul style="list-style-type: none"> • 67% enterprises spend 4%+ of revenue on IT; ~33% earmark >30% of IT budgets for digital spend • 97% enterprises increased spending on foundational digital technologies – Cybersecurity, Cloud, and Big Data Analytics
 <p>Increasing internet penetration</p>	<ul style="list-style-type: none"> • Internet penetration is growing at a CAGR of ~ 5% in India, expected to reach 78% penetration by 2027
 <p>Initiatives aimed towards digital India</p>	<ul style="list-style-type: none"> • Indian govt has rapidly adopted digital platforms for e-governance initiatives like UPI, CoWIN, Digilocker, etc.
 <p>Growing demand for professionals</p>	<ul style="list-style-type: none"> • Rapid increase in the job opportunities in the IT and digital sector to drive spending
 <p>Evolving consumer preferences after COVID</p>	<ul style="list-style-type: none"> • Changing consumer preferences in banking (contactless payments), FS and e-commerce • COVID triggered digital transformation and legacy modernization in India - remote working, automation, AI, etc.

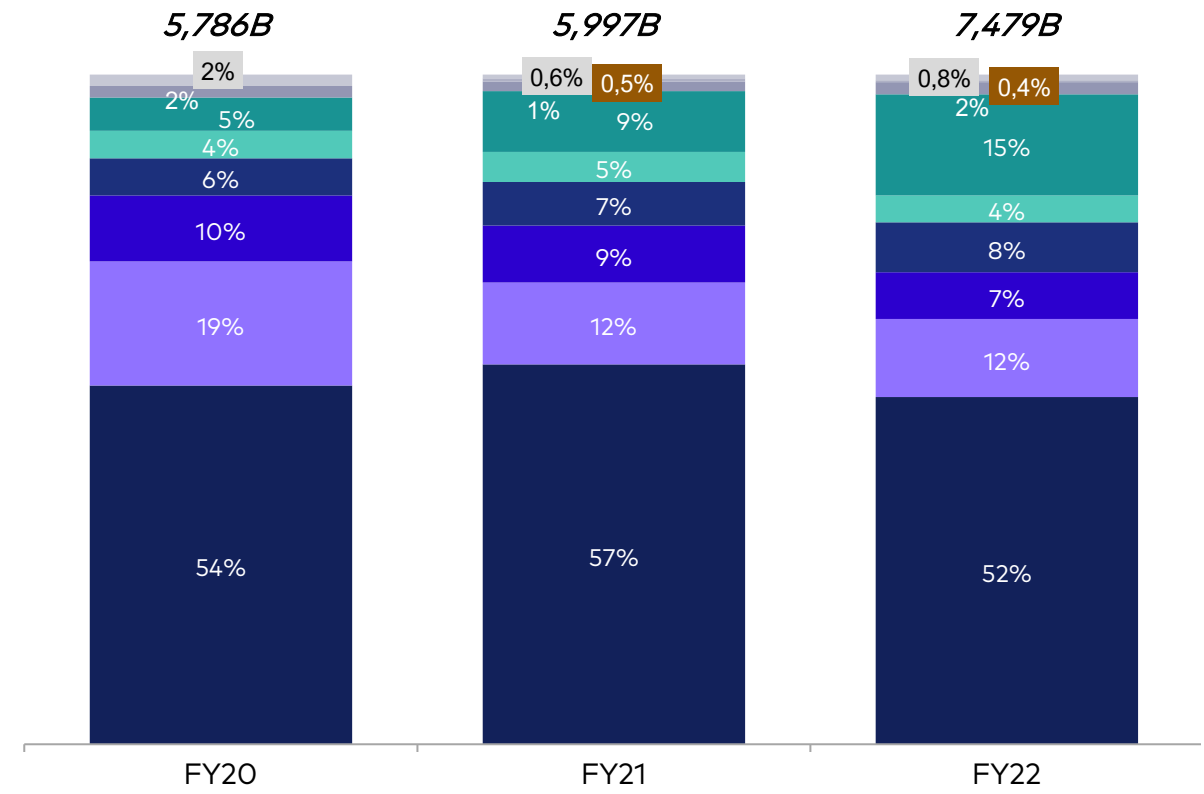
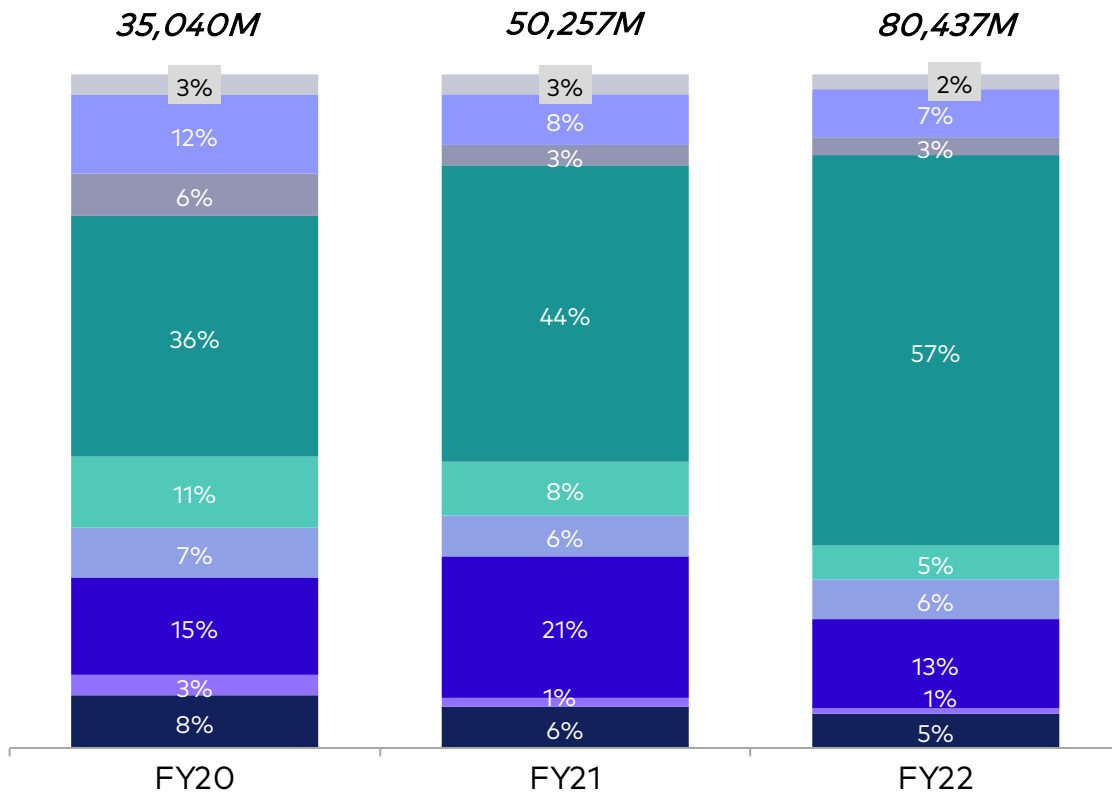
UPI holds the largest share (~57%) in total digital transaction volume but constitutes ~15% in digital transaction value owing to low ticket sizes

UPI accounted for ~57% of transaction volumes in FY22, followed by debit cards at ~13%

Digital retail transactions increased to US\$ 7.5T in FY22 as compared to US\$ 6T in FY21

Non-cash retail transactions – volume share
%, FY20 - 22

Non-cash retail transactions – US\$ Value share
%, FY20 - 22



Legend: NEFT, CTS, Debit card, IMPS, NACH, UPI, Credit card, M - wallet, Others

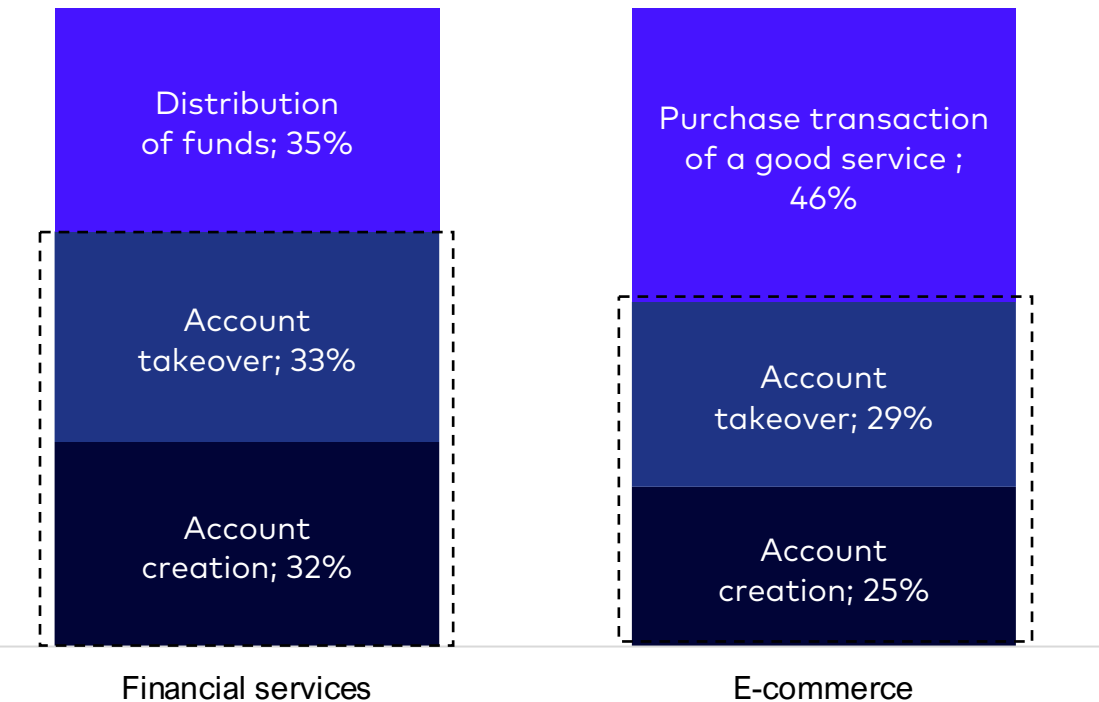
Note(s): US\$ 1 = INR 74
Source(s): NPCI data, Praxis analysis

Identity-related fraud: Account-related fraud holds a significant share; customer journey verification, balance between security and CX are the top challenges faced in detecting fraud

Account-related fraud holds ~65% share in financial services and ~54% share in e-commerce

Verification of customer journey and balancing fraud prevention with frictionless CX are some of the major challenges in detecting fraud

Identity related fraud distribution by activity
In %, 2021



Percentage of organizations using data analysis techniques
%, 2021



Source(s): LexisNexis report (survey of risk and fraud executives N = 418), Industry reports, Secondary research, Praxis analysis

Transaction-related fraud: FDP solutions can help in detecting and mitigating transaction-related fraud in banks; lack of data, frequently changing fraud patterns are key challenges

The highest number of fraud happens in advances (3,800+) followed by cards / internet (3,500+)

Area of operation	# of fraud (FY22)	Amount involved (in US\$ M, FY22)
Advances	3839	7353
Off-balance sheet	21	136
Foreign exchange transactions	7	1
Card / Internet	3,596	20
Deposits	471	62
Cash	649	12
Cheques / Demand drafts etc	201	20
Clearing accounts	16	0.1
Others	300	13

Note(s): Reporting period is FY 2020-21; Data is in respect of fraud of INR 0.1M and above reported during the period; US\$ 1 = INR 79.33
Source(s): RBI, Industry reports, Secondary research, Praxis analysis

Limited data, changing fraud patterns, system integration complexity are some of the key challenges faced by banks



Limited access to data points: Lack of enough historical data and challenge of richness of data, make blocking fraudulent payments complex and lead to high rates of false positives



Changing fraud patterns over time → decrease in the fraud detection and prevention model's performance and efficiency



Incorrect / incomplete data: Non - submission of reports by the customers and non-sharing of information → difficulty in integrating data and identifying fraud



Complexity in system integrations: Most of the traditional cooperative banks have outdated internal systems which can't integrate with new-age AI FDP solutions



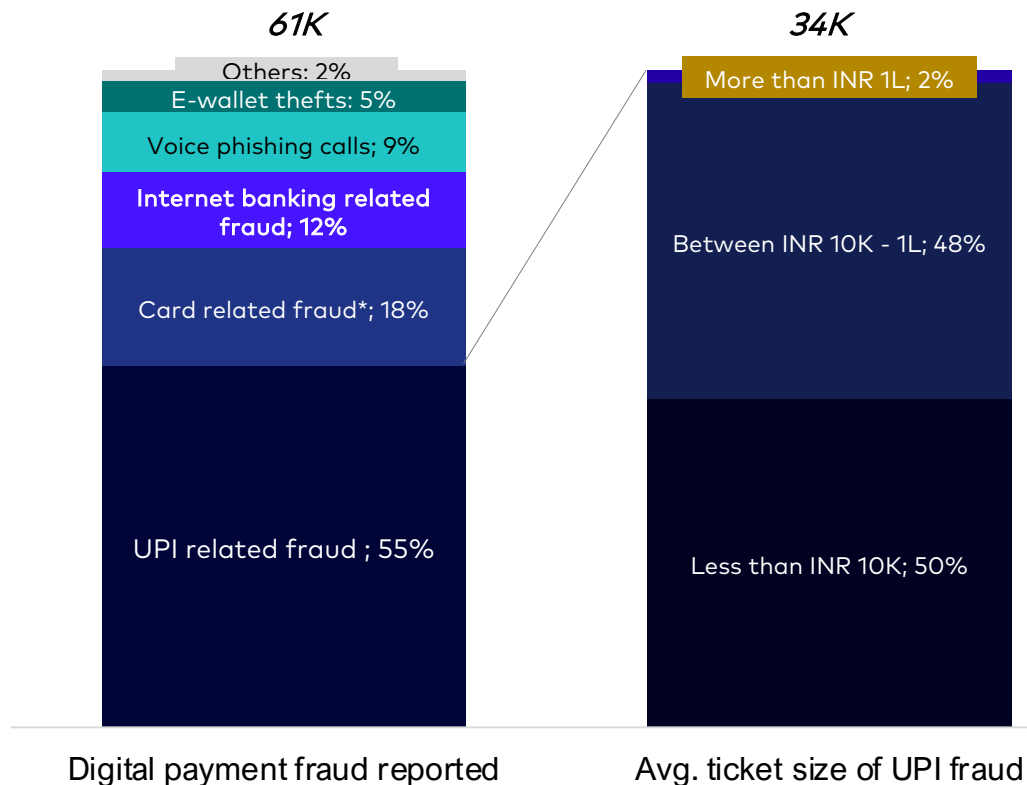
Balancing CX and security against fraud: It is important to make the process of onboarding smooth and frictionless to retain customers, while not losing out on the security








Of the total reported digital payment fraud, ~55% are UPI – related; Half of the UPI – related fraud are of low ticket size (less than INR 10K)

UPI - related fraud constituted ~55% of the total digital payment fraud in May 2022

Phishing, vishing, malware, deceptive UPI handles are some of the most prevalent UPI scams

Monthly UPI fraud
In %, May 2022



 Phishing	<ul style="list-style-type: none"> Fraudsters send bogus emails to access sensitive information (password or PIN) of the potential victim
 Malware	<ul style="list-style-type: none"> Malware is designed to extract and copy data from the infected device It can be mistakenly downloaded from a fake e-mail attachment or an unsecured website
 Vishing	<ul style="list-style-type: none"> Fraudsters contact individuals claiming to be bank employees, asking for a UPI pin, or requesting to download a third-party app for verification purposes
 Deceptive UPI handles	<ul style="list-style-type: none"> Fraudsters create fake UPI handles on social media to trick people into revealing account details
 Remote screen monitoring	<ul style="list-style-type: none"> Downloading an unverified app from the app store can sometimes result in a privacy breach and data leak
 Money mule accounts	<ul style="list-style-type: none"> More sophisticated scam in which fraud rings get the victim's data and then transfer money to an intermediary account to store the plunder
 SIM cloning	<ul style="list-style-type: none"> SIM cloning is a recent addition that has proliferated post the OTP-mandatory rule by banks A fraudster can even modify the UPI PIN if he/she clones the SIM

Note(s): * Debit / credit card, swapping of mobile phone SIM cards
Source(s): Industry reports, RBI data, Secondary research, Praxis analysis

Government of India has passed key regulations that is expected to drive spend on FDP solutions

Regulations / Initiatives	Brief description	How can FDP solutions help?
Two-factor / additional factor of authentication	<ul style="list-style-type: none"> RBI has raised the Additional Factor of Authentication (refers to a pin or an OTP) limit from INR 5,000 to INR 15,000 per transaction for e-mandates on cards, Prepaid Payment Instruments (PPIs), and UPI for recurring transactions 	<ul style="list-style-type: none"> FDP solutions provide various authentication techniques – behavioral, physical authentication, etc.
Central registries	<ul style="list-style-type: none"> Multiple registries like Central fraud registry (CFR), Centralized KYC registry (CKYCR), Central payments fraud information registry (CPFIR), etc. have been set up for data and fraud – related information reporting 	<ul style="list-style-type: none"> FDP platforms help in comprehensive capturing of data, which enables efficient reporting
Mandate for reporting of fraud to RBI	<ul style="list-style-type: none"> Banks need to furnish Fraud Monitoring Return (FMR) in individual fraud cases, irrespective of the amount involved, to RBI electronically within three weeks from the date of detection 	<ul style="list-style-type: none"> FDP platforms help in easy and real-time data collection → improved auditability
Mandate for monitoring fraud	<ul style="list-style-type: none"> Banks are required to constitute a special committee for monitoring and follow up of cases of fraud involving amounts of INR 1Cr and above exclusively, while the Audit Committee of the Board (ACB) may continue to monitor all the cases of fraud in general 	<ul style="list-style-type: none"> FDP platforms have a suite of solutions to detect and prevent fraud of all transactions irrespective of its value
Separate department to manage fraud	<ul style="list-style-type: none"> The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an independent group in the bank 	<ul style="list-style-type: none"> Through FDP solutions, fraud department can easily and effectively manage and track fraud
Regulatory framework	<ul style="list-style-type: none"> RBI has mandated that all types of loans irrespective of tenor or size need be reported to credit bureaus The RBI would set up baseline technology standards for DLAs that would strengthen cyber security, data protection and prevent fraud like loan disbursement on stolen identity, data breaches, etc. 	<ul style="list-style-type: none"> FDP systems aid in the thorough data collection, enabling effective reporting
KYC process and periodicity of Re-KYC	<ul style="list-style-type: none"> IRDAI has mandated KYC for all insurers with defined documents, process and flows Periodicity for Re-KYC for low risk and high risk is set to once in 2 years and every year respectively 	<ul style="list-style-type: none"> FDP systems will not only provide authentication techniques but will also keep a track of the periodicity for Re-KYC digitally
Suspicious transaction report	<ul style="list-style-type: none"> IRDAI has stressed to put more focus on STR, alerting and understanding money laundering threats 	<ul style="list-style-type: none"> FDP systems will aid tracking and generation of suspicious transaction report
Open banking initiatives	<ul style="list-style-type: none"> Open banking has been promoted with the launch of intermediary AAs (account aggregators), responsible for the customers' consent management → increased financial transparency, reduced fraud with respect to forged documents 	<ul style="list-style-type: none"> FDP provides comprehensive third-party data (open access to consumer banking, transaction, and other financial data from banks, NBFCs) → improved transparency and richness of data

Note(s): Information as of August 2022

Source(s): RBI guidelines, Industry reports, Secondary research, Praxis analysis

Cost of fraud to company varies between 3X and 5X of fraud value in key verticals; web browser channel accounts for more than 40% of fraud costs in India

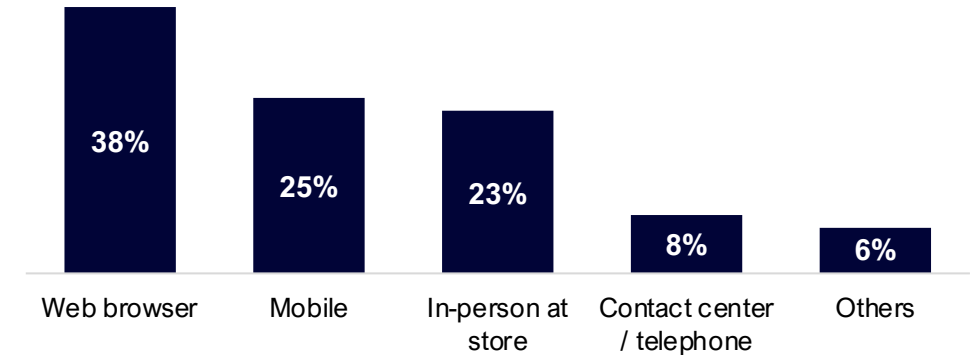
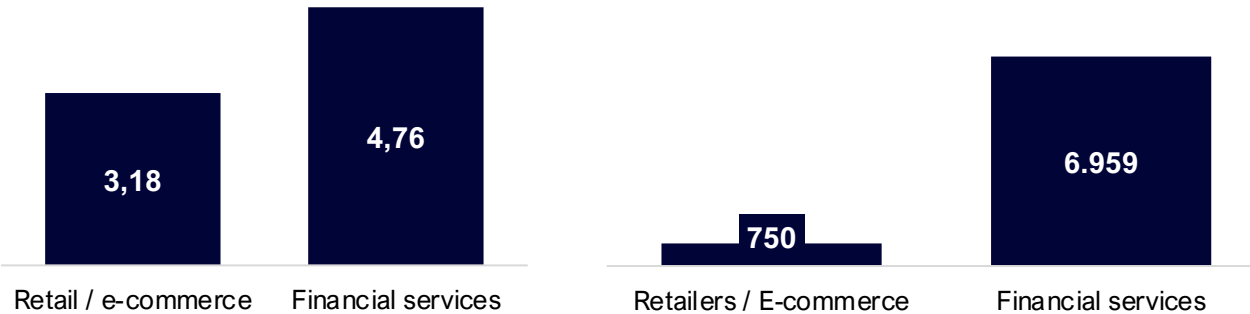
Fraud costs ranges between 3 - 5 times fraud value; Average value of fraud attacks in FS is close to 10x of that in e-commerce

Web browser channel accounts for the single largest source of fraud costs in India

Cost of fraud per unit US\$ loss in transaction

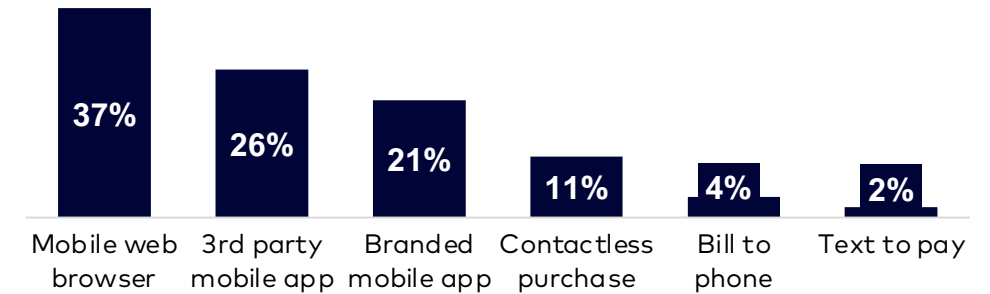
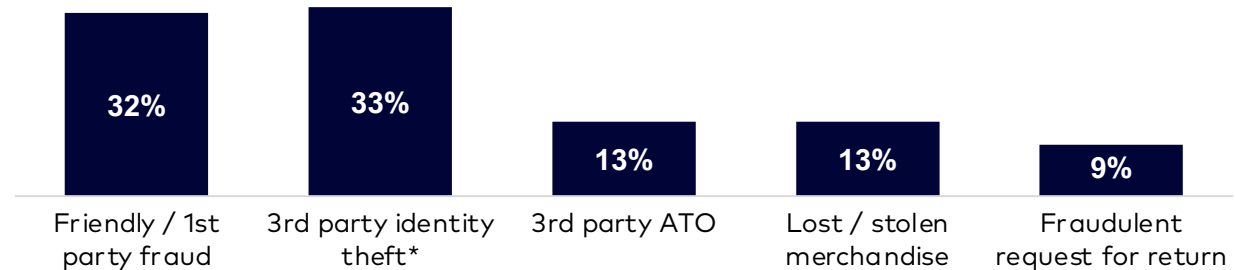
Avg value of successful fraud attacks¹ In US \$

% fraud costs by channel In %, 2021



Distribution of losses by fraud type In %, 2021

% fraud costs by mobile channel In %, 2021

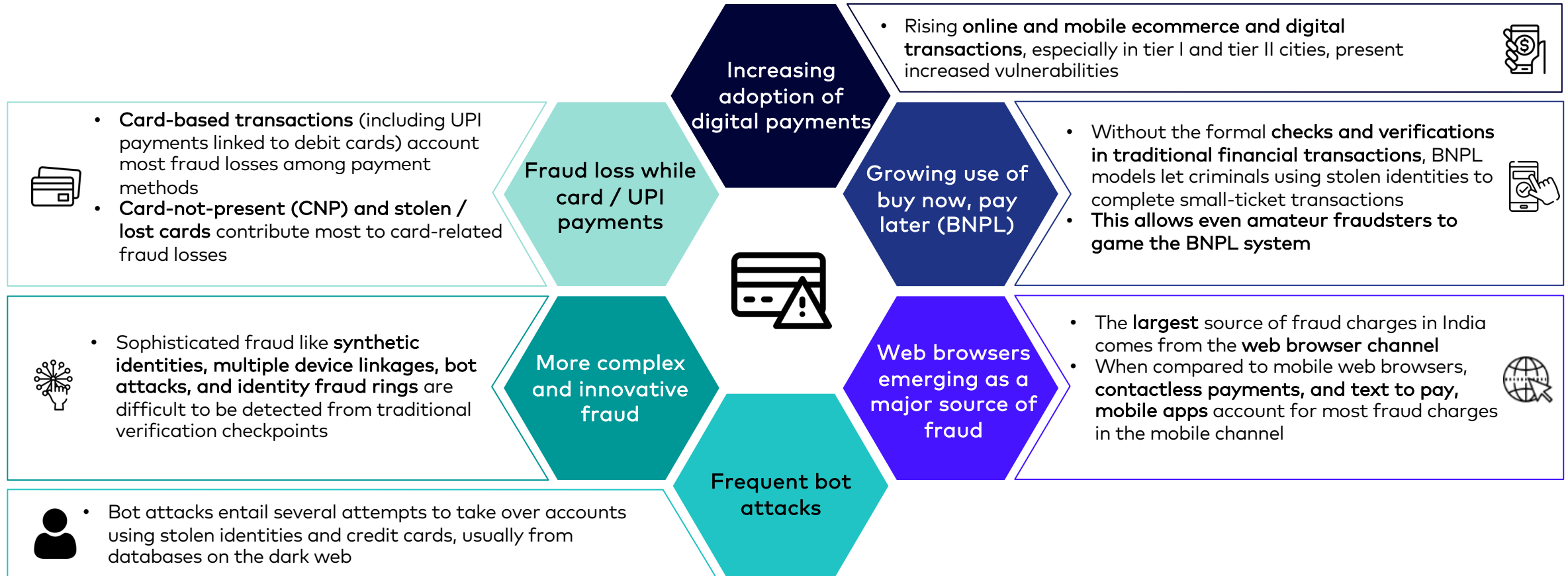


Source(s): LexiNexis (Survey of N=108 fraud and risk executives across industries), Industry reports, Secondary research, Praxis analysis

Note(s): * Also includes synthetic identity fraud; 1. May increase or decrease based on seasonality; 2. 3rd party apps connect with another service (for payments etc); 3. Branded mobile apps are created by company to promote its brand and are owned by the company; 4. Contactless purchases are payments use contactless enabled payment terminals (NFC enabled devices) to complete transactions

Pandemic has accelerated the need for advanced FDP solutions owing to the increase in exposure to digital fraud

Emerging fraud trends



Source(s): Lexis Nexis India report (survey N = 108), Industry reports, Secondary research, Praxis analysis

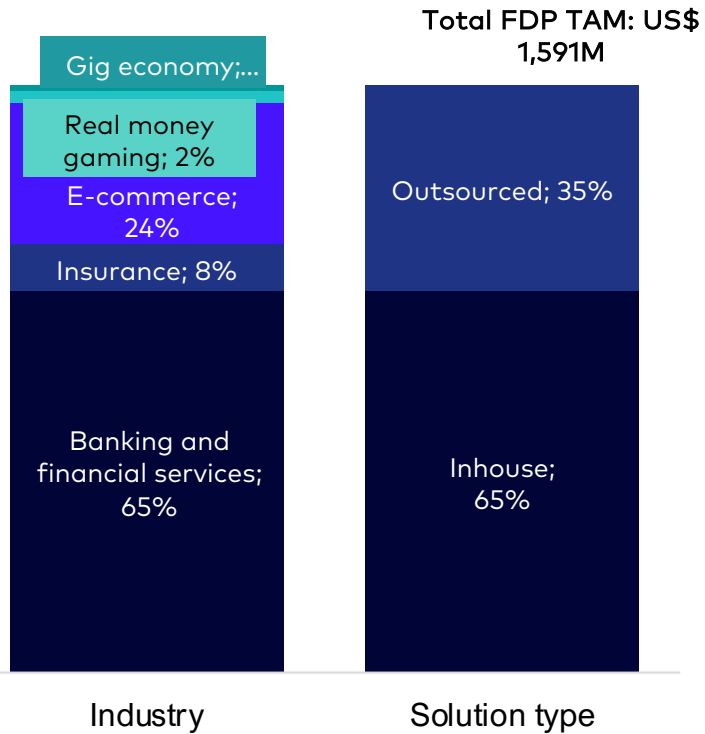
FDP TAM was US\$ 1.5B+ in 2022 and is growing at a CAGR of 37%; FDP SAM market was US\$ 550M+ in 2022 and is expected to be US\$ 3,068M by 2027, growing at a CAGR of ~41%

BFSI hold the largest share (73%) followed by e-commerce (24%)

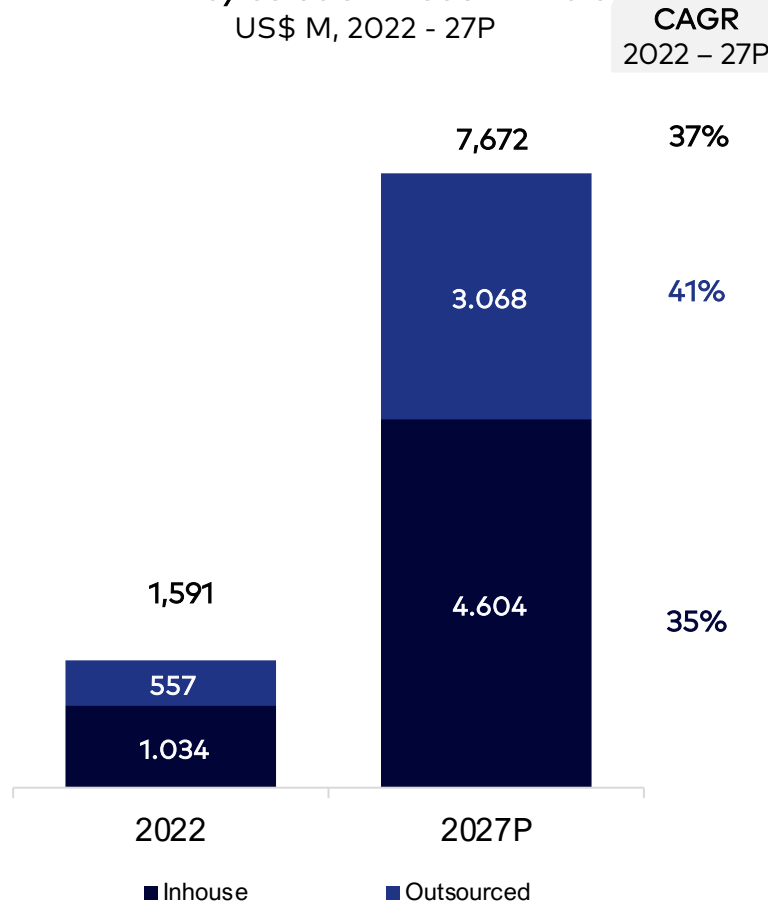
FDP TAM stood at US\$1.6B in 2022 and is expected to be US\$ 7.6B+ by 2027

Rising digitization, govt. initiatives aimed towards increasing security driving adoption

FDP TAM split across industries, solution types, 2022



TAM by solution model in India US\$ M, 2022 - 27P

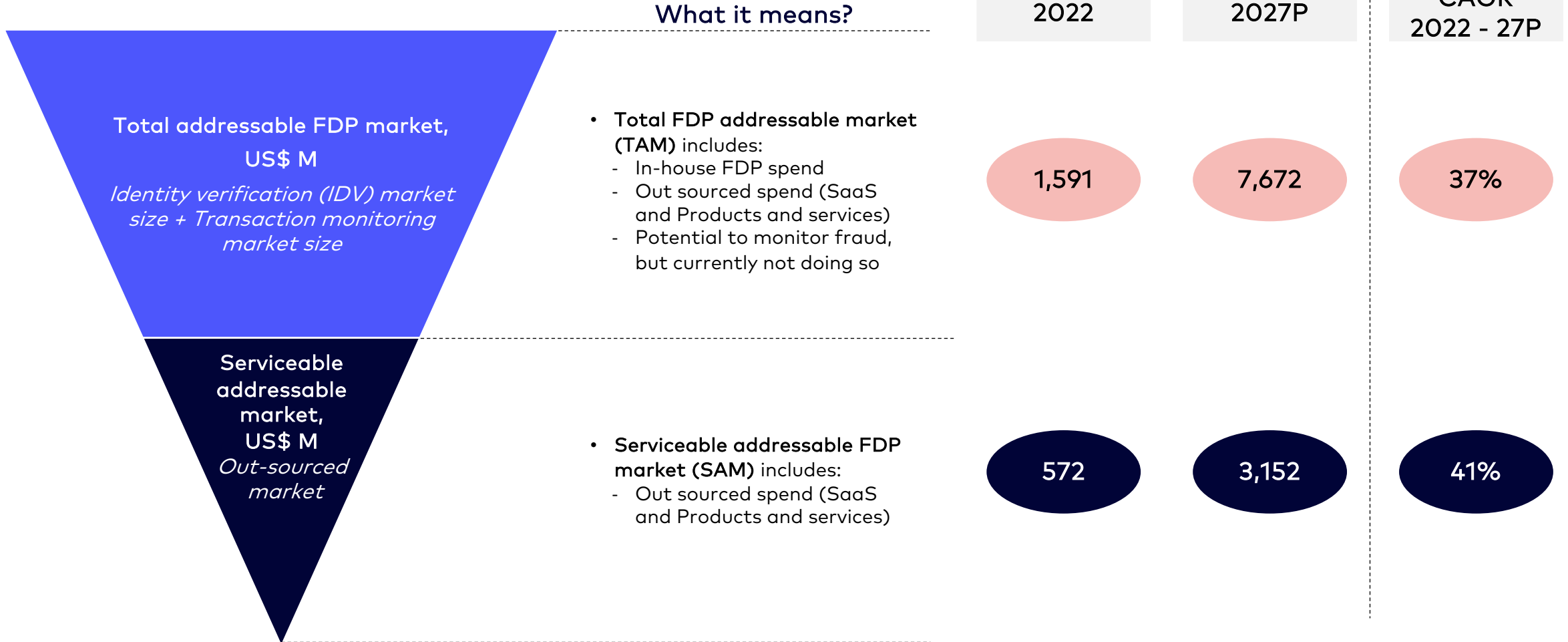


Growth factor	Details
Increasing digitization	<ul style="list-style-type: none"> India's IT spending is expected to reach US\$ 160 B in 2027, growing at a 9% CAGR Spend on SaaS is expected to increase at the highest rate of 16% between 2022-27
Evolving consumer preferences post COVID	<ul style="list-style-type: none"> COVID triggered digital transformation and legacy modernization in India - remote working, focus on automation, AI, cybersecurity etc.
Govt initiatives	<ul style="list-style-type: none"> Regulations like 2-factor authentication, Central fraud registry (CFR) and data privacy policies to augment the adoption of FDP solutions in India
Growing number of digital-first businesses	<ul style="list-style-type: none"> Businesses across sectors are taking a digital route to growth 2x growth in micro businesses actively transacting online Digital-first businesses allowing consumers to transact online, will require to develop FDP solutions in the near future
Increasing internet penetration	<ul style="list-style-type: none"> Internet penetration is growing at a CAGR of ~ 5% in India, expected to reach 78% penetration by 2027 Increasing deployment of Fibernet and internet lines in rural India

Source(s): Industry reports, Primary conversations, Secondary research, Praxis analysis

Total FDP SAM stood at US\$ 570M+ in 2022 and is projected to be ~US\$ 3,152M by 2027, growing at a CAGR of 41%

Total addressable FDP market in India was US\$ 1.5B+ whereas the FDP SAM was US\$ 570M+ in 2022



Source(s): Industry reports, Primary conversations, Secondary research, Praxis analysis

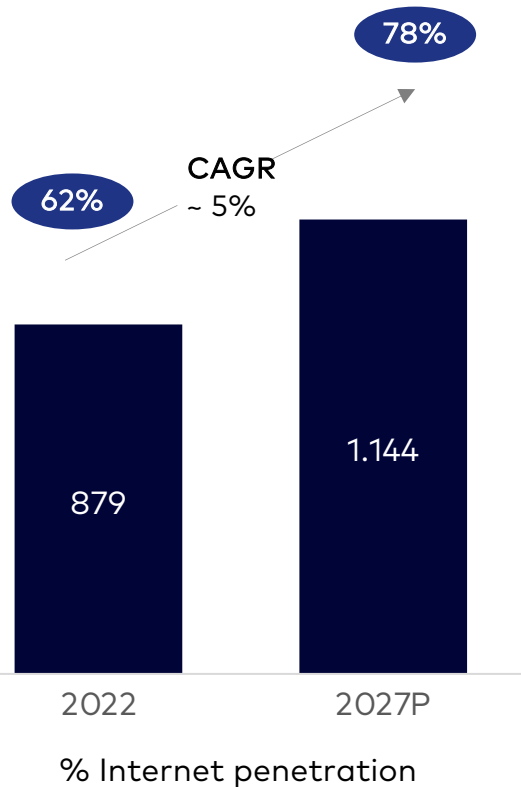
Indian consumers prefer transacting online or through mobile, with internet penetration increasing to 78% by 2027

Internet users are expected to reach 1,144M in 2027

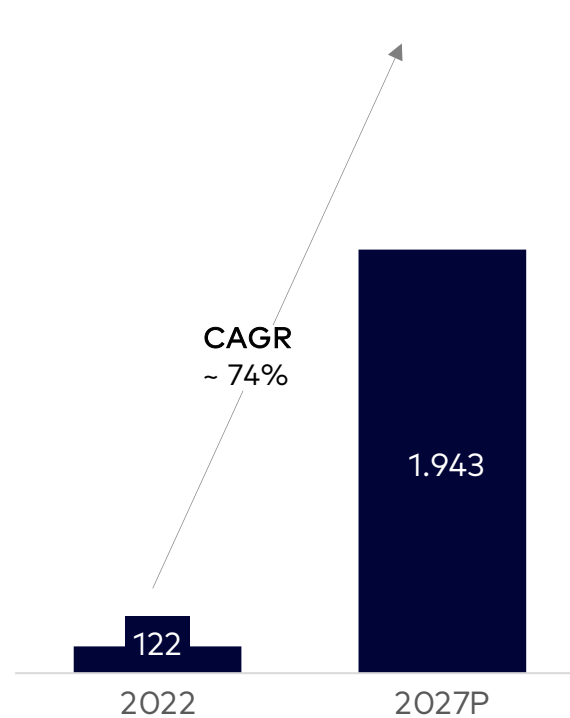
Digital payments are expected to grow at a CAGR of 74% b/w 2022-27






Expanding digital commerce, adoption of digital native products leading to increase in digitalization

of internet users in India
M, 2022 - 27P



Digital payments in India
B, 2022 - 27P



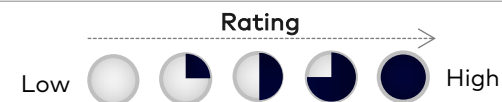
 <p>Expanding digital commerce</p>	<ul style="list-style-type: none"> Digital commerce – both eCommerce and m-commerce – is estimated to expand significantly eCommerce expected to grow at 35-40% CAGR and m-commerce clocking 25-27% CAGR through 2025
 <p>Adoption of digital native products</p>	<ul style="list-style-type: none"> India's new middle class will seek more digital-native and personalized products and services, will drive digital payments Reduced cost of mobiles, ease of use and increased value is driving consumers to buy digital devices
 <p>Increasing internet penetration</p>	<ul style="list-style-type: none"> Internet penetration is growing at a CAGR of ~ 5% in India, expected to reach 78% penetration by 2027 Increasing deployment of Fibernet and internet lines in rural India
 <p>Regulatory changes</p>	<ul style="list-style-type: none"> Regulatory sandboxes by RBI to innovate on low-cost, mass-inclusion solutions will be a big boost to digital payments Govt's drive to control voice and data costs – emergence of 5G
 <p>Facilitation of ease of availing services</p>	<ul style="list-style-type: none"> Basic services like bank account opening, transferring and receiving money, company registration, media consumption now happens on mobile easily – driving demand for digitization

Note(s): World bank data has been leveraged while taking population estimates; 1. EFT: Electronic Fund Transfer
Source(s): RBI, World bank, NAASSCOM, Secondary research, Praxis analysis

Companies in Banking and financial services, Insurance and Gaming sectors typically develop in-house FDP solutions

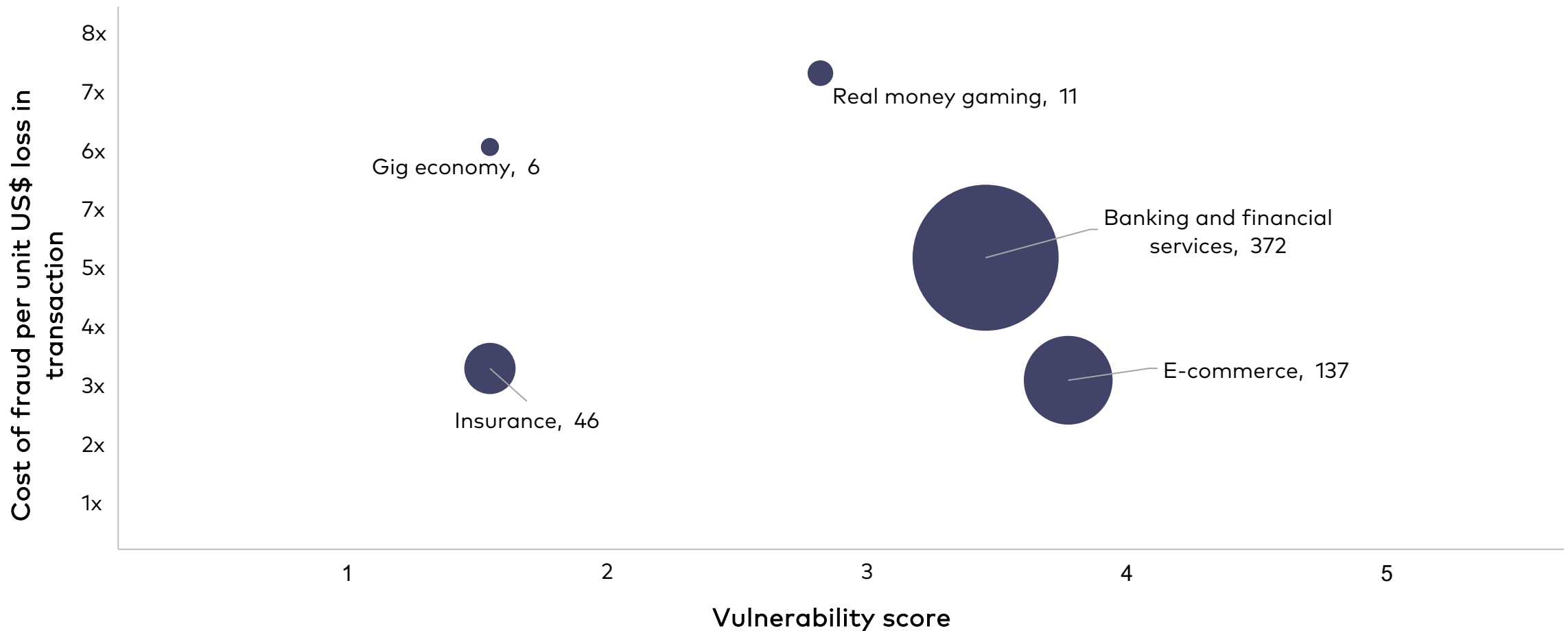
	Banking and financial services	Insurance	E-commerce	Gaming	Cryptocurrency	Gig economy
Capabilities	<ul style="list-style-type: none"> Email intelligence Phone intelligence Document verification Behavioral biometrics Orchestration Device fingerprinting 	<ul style="list-style-type: none"> Web authentication Frictionless authentication OCR, face match, name match Email, phone and device intelligence Device fingerprinting 	<ul style="list-style-type: none"> Device intelligence Purchase / Affluence intelligence Document verification 	<ul style="list-style-type: none"> WebAuthn Frictionless authentication Document verification Face match 	<ul style="list-style-type: none"> Behavioral biometrics WebAuthn Document verification Device intelligence Orchestration 	<ul style="list-style-type: none"> Behavioral biometrics OCR Trust network Device fingerprinting Sections intelligence
Use cases	<ul style="list-style-type: none"> User authentication Document validation User risk profiling AML monitoring Account takeovers Self - service onboarding 	<ul style="list-style-type: none"> User authentication Document validation User risk profiling Agent abuse Account takeovers Self - service onboarding 	<ul style="list-style-type: none"> RTO predictions Returns prediction Chargeback prevention AML monitoring 	<ul style="list-style-type: none"> User authentication Document validation User risk profiling Fake accounts Account takeovers Self - service onboarding 	<ul style="list-style-type: none"> User authentication Document validation Fake accounts Account takeovers Self - service onboarding 	<ul style="list-style-type: none"> User authentication Document validation Account takeovers Promo abuse Self - service onboarding
Native product capability						
In-house						
API Call - SaaS driven						
Outsourced integration services						

Source(s): Industry reports, Secondary research, Praxis analysis



Banking and financial services and e-commerce are the most vulnerable industries with respect to fraud attacks

Cost of fraud per unit US\$ loss in transaction with respect to spend on FDP
2022



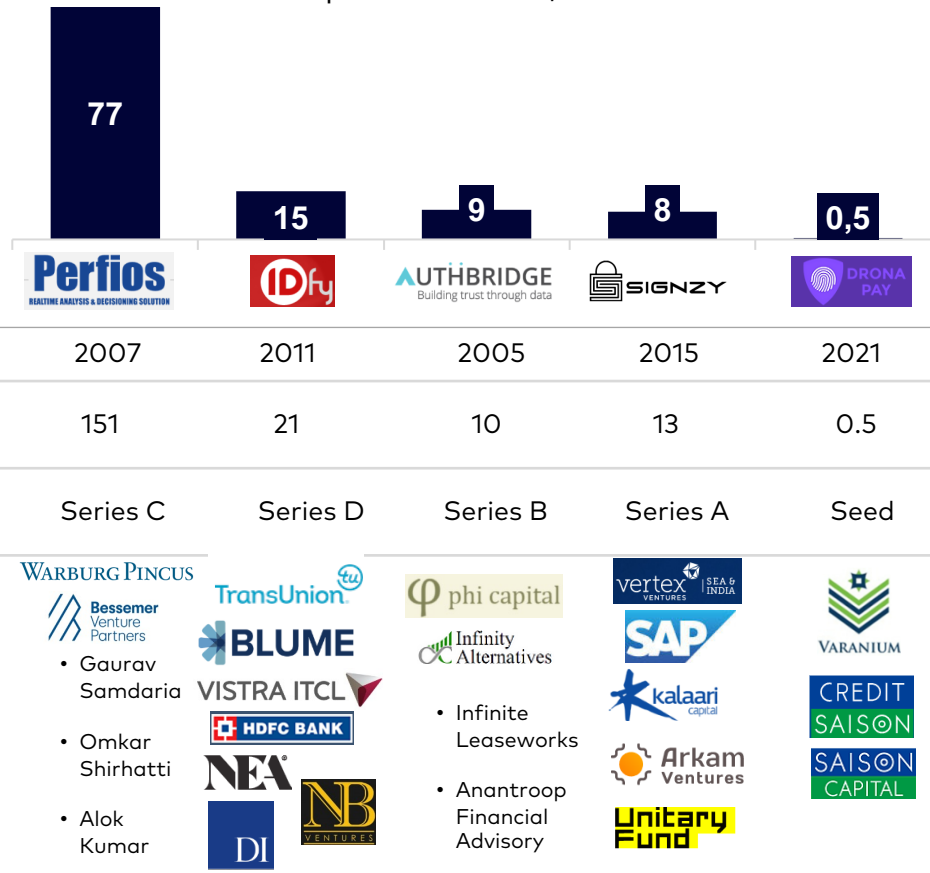
Note(s): *Vulnerability score (on a scale of 0 to 5) is estimated basis parameters like the number of touchpoints susceptible to fraud attacks, number of active users, impact of regulation, etc.
Source(s): Primary conversations, Secondary research, Praxis analysis

● SAM of FDP for respective industries (in US\$ M)

Several FDP companies have raised funding since April 2020; capabilities enhancement is one of the prime reasons for strategic acquisition of FDP players

Multiple investments can be seen in FDP players since April 2020; Perfios has raised US\$ 77M+ funding in last two years

Key investments in FDP players
Apr'20 – Mar'22, US\$ M








Large players acquire FDP firms to enhance their capabilities and to enrich their existing portfolio

Acquirer	Target	Acq. year	Rationale
		2022	<ul style="list-style-type: none"> To bolster its approach to providing a comprehensive platform for financial institutions – a fully integrated technology stack, including identity and onboarding services
		2022	<ul style="list-style-type: none"> To strengthen its lending-focused product offerings
		2019	<ul style="list-style-type: none"> To expand advanced bot protection capabilities
		2019	<ul style="list-style-type: none"> To improve its cloud security portfolio To enhance anti-bot and fraudulent traffic protections

FDP SaaS players focus largely on product development by building their tech stack and partnerships with IT service providers

Advanced AI / ML, biometrics, real-time monitoring, blockchain are key components of FDP products

 <p>AI powered KYC</p>	<ul style="list-style-type: none"> • Bank Secrecy Act (BSA) engines - Automated bank statement analyzers to detect and prevent fraudulent activities while onboarding
 <p>Multi-factor authentication and biometrics</p>	<ul style="list-style-type: none"> • Combine physical and behavioral biometrics like hand geometry (hand gesture and movements), keystroke analysis, etc. to create a robust security solution using AI
 <p>Real-time monitoring</p>	<ul style="list-style-type: none"> • Advanced real-time transaction monitoring and instant notification
 <p>Blockchain technology</p>	<ul style="list-style-type: none"> • Blockchain contains digital assets including documents that are secured via powerful cryptographic keys, hence making it more secure
 <p>Predictive analytics</p>	<ul style="list-style-type: none"> • FDP players use predictive analytics to detect potential security threats and to establish patterns in high-crime areas, among other activities

FDP players develop efficient partnership network for sourcing data and detecting and investigating fraud



- | | |
|---|--|
| <ul style="list-style-type: none"> • Government (for RBI database) • Bureaus • Aggregators like website builders • Global data partners | <ul style="list-style-type: none"> • Technology partners • Telcos (for IT proofing) • Cloud services • Email intelligence service provider |
|---|--|



Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Frictionless CX with robust security, unavailability of data are the main challenges faced by FDP players; digitalization, growth in fintech startups are the major drivers

Headwinds / Challenges



Balancing speed of detection with customer friction: Offering a robust security solution with minimum customer friction is a challenge



Lack of quality data to support analysis: Data quality is a challenge, specifically with respect to customers and transactions → **inefficient monitoring mechanisms**



Creating awareness regarding fraudulent activities. Companies focus on KYC compliance but not on fraud management



Heavy investments into **AI / ML** training and tuning models



Security risks: Clients are reluctant to share their confidential data with the FDP solution provider. **Building relationships and trust** is a challenge for FDP players

Tailwinds / Opportunities



Accelerating digitalization: Internet users in India are 879M+ in 2022 and are expected to **cross 1,144M by 2027**. Digital payments are increasing dramatically from 122B in 2022 to 1.9T+ in 2027, growing at a **CAGR of 74%**



2100+ fintech companies in India which are one of the largest adopters of FDP solutions → greater opportunity for FDP players



Lack of expertise in different types of fraud: fraud are becoming a **more complex and sophisticated** → need for external expert support in identifying and preventing



Tech capabilities crunch: Handling and developing a FDP solution requires technical capabilities and talented resources which is a challenge for most organizations → **greater potential for FDP players**



Government regulations like authentication mandates, KYC, etc. are driving the adoption of FDP solutions

Source(s): Primary conversation, Industry report, Secondary research, Praxis analysis

High fraud detection accuracy, real-time monitoring, and ease of integration are the key criteria influencing the purchase of FDP solutions

Most important	Purchase criteria	Sub criteria	Customer rating
Relatively less important	Features	<ul style="list-style-type: none"> Fraud detection accuracy Real-time tracking of transactions with automated decisions Shortest response time Customizability / configurability Chargeback guarantee End-to-end solutions or orchestration capability Ability to handle the scale of transactions 	
	Cost	<ul style="list-style-type: none"> Pricing model <ul style="list-style-type: none"> Deployment cost Monthly fees or subscription model Micro fees based on API calls Free trial and proof of concept 	
	User experience	<ul style="list-style-type: none"> Ensuring customer education and awareness through meaningful SMS and emails sent at regular intervals to mitigate customer vulnerability 	
	Integration and support	<ul style="list-style-type: none"> Ease of integration of the FDP platform with existing tech tools Support and training for smooth integration 	
	Vendor reputation	<ul style="list-style-type: none"> Reliability and credibility Post-sale support Reputation & customer reviews Recommendation from peers 	

"For our company, real-time tracking of transactions and blocking fraudulent transactions when identified is a very important feature. Automated decisions by the platform is an also important factor."

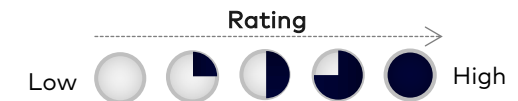
- Fraud prevention manager, E-commerce

"We integrated with an FDP SaaS product to introduce of multifactor authentication (MFA) with integrated biometrics to ensure the user account is not hacked or used by others without user consent"

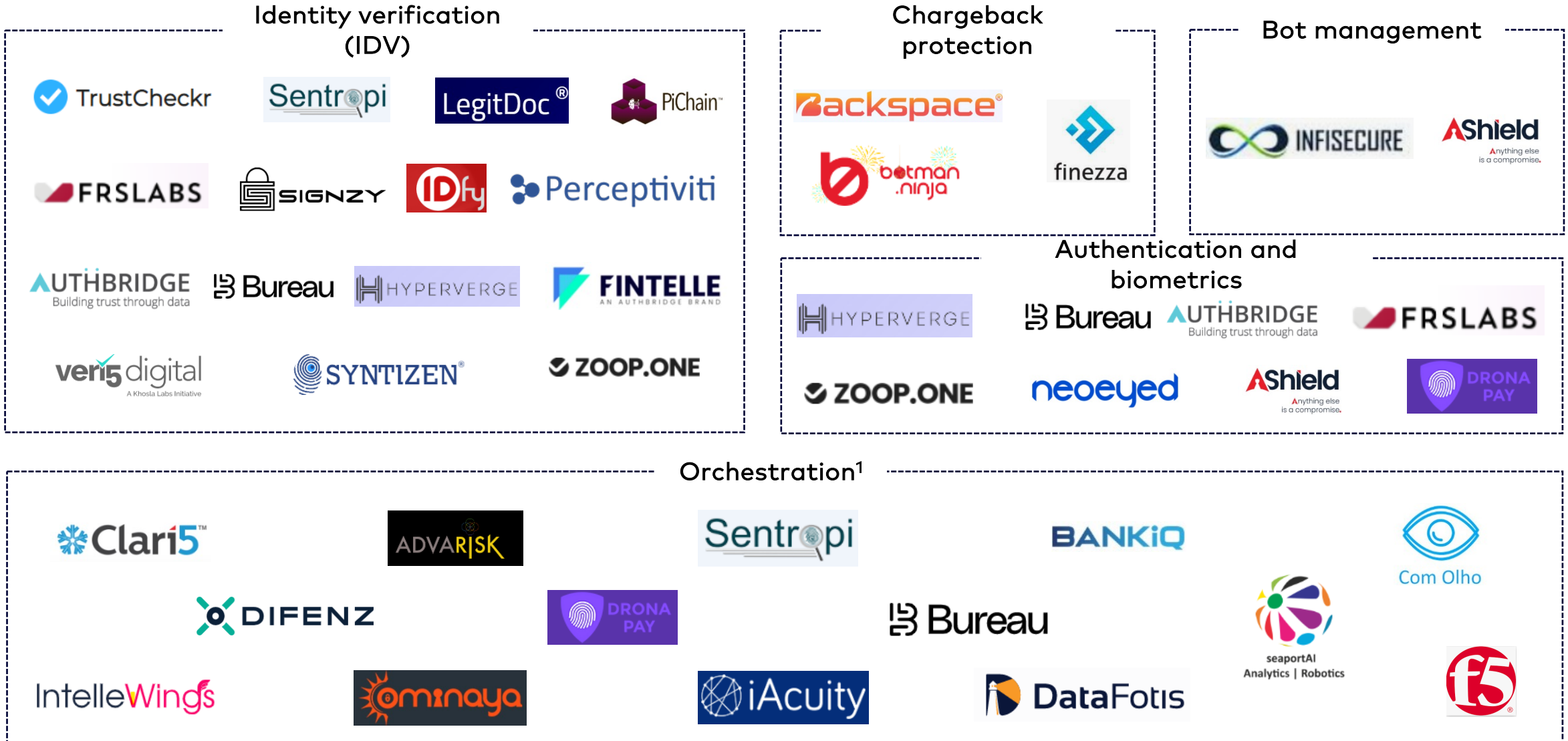
- Product manager, BFSI

"Fraud detection is a new area for us; hence we did our background research to find the best FDP tool in the market by recommendations from our colleagues and other industry players"

- Product manager, E-commerce



FDP landscape is evolving rapidly in India



Note(s): 1. A solution that connects tools producing risk and trust signals to underlying analytics tools, and provide step-up authentication in response; This is not an exhaustive list
 Source(s): Industry reports, Secondary research, Praxis analysis

Founded in 2020, Bureau offers end-to-end risk compliance, and identity management solutions for businesses [1/2]



Founded
2020



Headquarters
San Francisco



60+
Employees

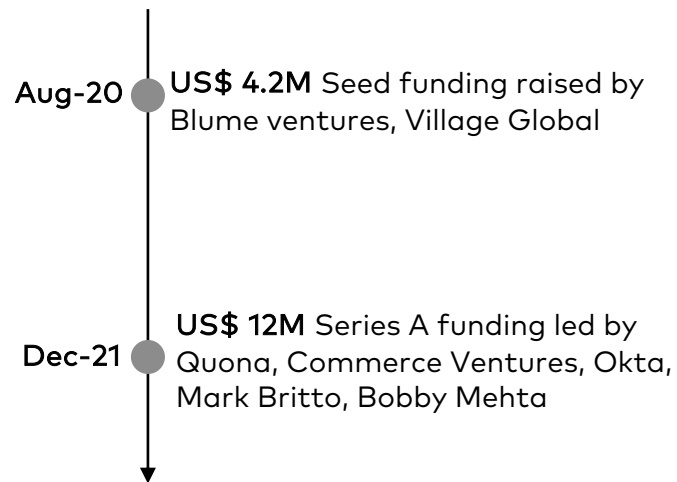


Total funding
US\$ 16.2M
(Series A)



Overview
Offers risk compliance, and identity management solutions for businesses

Funding timeline



Key highlights

50m+

Verified Identities

500+

Risk Signals

\$300m+

Commerce Protected

50m+

API Calls

80+

API

Strengths

- Identity and risk orchestration to automate every onboarding, transaction, and fraud-risk decision
- Workflows for user journey mapping and control with all the data and building blocks
- **AI-powered** business rules engine to define business logic and determine outcomes
- Bureau platform facilitates **multiple vendor management** under one roof, thus reducing the tool debt
- **Global coverage** from day 1 to support multi-geography operations
- **Reduced manual reviews** and **streamlined compliance and audits**
- **Easy integration** with any tech stack that requires sparse tech bandwidth

Platform features

No code workflows	Customized workflows from hundreds of data sources
Templates	Ready-to-go templates catering to different industries and use cases
Data ingestion	Generate complicated insights on the platform using bulk uploads
Rules engine	Advance AI-based engine to deploy complex business logic
Case management	Review flagged cases and manage compliance
Reports	Granular insights to enhance fraud detection & promote real-time responses

Note(s): Information as of Nov 2022
Source(s): Company websites, Secondary research, Praxis analysis

Founded in 2020, Bureau offers end-to-end risk compliance, and identity management solutions for businesses [2/2]

Types of use cases



User onboarding

KYC

AML and compliance

Risk management

Transaction monitoring

Fraud prevention

Robust risk assessment at onboarding using **Bureau's rich persona, KYC, device, and behavior insights**

Stay compliant with government regulations and make **better-informed decisions** about your users

Keep a **watchful eye** on the parking of illicit funds and stay compliant

Assess users at **every stage** in their customer journey to make informed decisions

Monitor account activity and transactions to flag suspicious activities

Stop fraudsters before they can abuse the system and result in financial and reputational loss

Note(s): Information as of Nov 2022
Source(s): Company websites, Secondary research, Praxis analysis

IDfy is a series D funded FDP player headquartered in Mumbai, with a revenue growth of 70% between FY19 - 22



Founded
2011



Headquarters
Mumbai



Total revenue
US\$ 7.8M (FY22)



Total funding
US\$ 21M
(Series D)



Offerings
Offers tools for identity verifications, BGV

Funding timeline

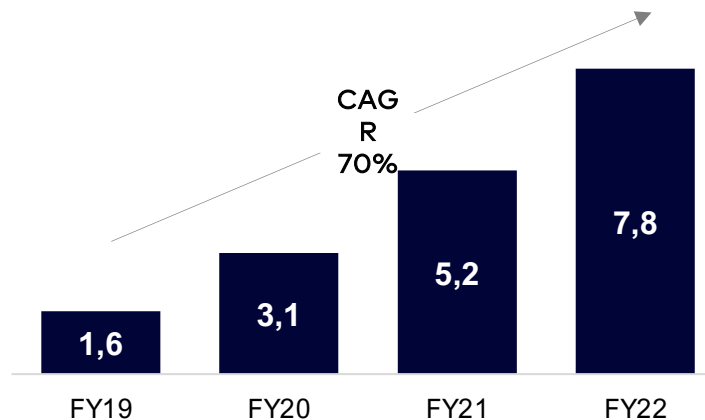


Strengths

- Proprietary systems are built on the latest in machine-learning based anomaly detection, machine vision, and identity authentication techniques
- Company is currently serving 200 clients across financial services

Financials

Revenue
US\$ M, FY19 - 22



Key solutions / services

Solution / service	Details
Customer verification	<ul style="list-style-type: none"> Ensure that the client has the right customers and they are onboarded in the fastest way possible
Employee verification	<ul style="list-style-type: none"> Help build honest and high performing teams by preventing identity and employment fraud through accurate and reliable employee verification
Partner verification	<ul style="list-style-type: none"> Ensure that the client's service partners are comprehensively verified and onboarded in the shortest time possible
Merchant onboarding	<ul style="list-style-type: none"> Help in onboarding merchants from remote corners while validating their business identity and proofs instantly
Video KYC	<ul style="list-style-type: none"> Makes remote onboarding safe

Note(s): Information as of July 2022
Source(s): Industry reports, Company websites, Secondary research, Praxis analysis

Clari5 offers cross-channel fraud management platform for banking enterprises



Founded
2006



Headquarters
Bengaluru



Total revenue
US\$ 5.7M (FY21)



Total funding
US\$ 4M
(Series A)



Overview
Offers a cross-channel fraud management platform for banking enterprises

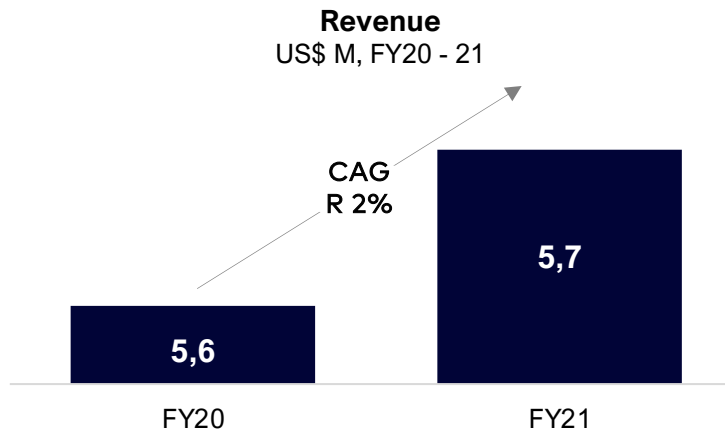
Funding timeline



Strengths

- Real-time, cross-channel platform offering **bottom - line protection (losses from fraud)** and **topline growth (cross - sell / upsell)**
- Capability to process **10B+ transactions** and manage **450M+ accounts**
- With **200M accounts** at a single site, it has the **world's largest** implementation of a fraud management solution

Financials



Type of solutions / technologies / services

Solution / service	Details
Enterprise fraud management	• Extreme real-time, cross channel Enterprise Fraud management to detect and prevent sophisticated internal and external fraud
Anti-Money Laundering	• End-to-end AML platform with Suspicious activity monitoring, customer risk categorization , entity identity resolution, watchlist filtering
Payments fraud reporting	• Unified, comprehensive, ready-to-deploy, single-point regtech platform for end-to-end automated payments
Customer experience management	• Extreme real-time, cross channel contextual insights to target customers for cross-sell and upsell
Identity resolution	• Minimise risk exposure with a real-time, unified customer view across all lines of businesses and products

Note(s): Information as of July 2022
Source(s): Industry reports, Company websites, Secondary research, Praxis analysis

Founded in 2015, Signzy offers a range of services like video KYC, fintech APIs, deep user analytics among other advanced features



Founded
2011



Headquarters
Mumbai



Total revenue
US\$ 4.7M (FY22)

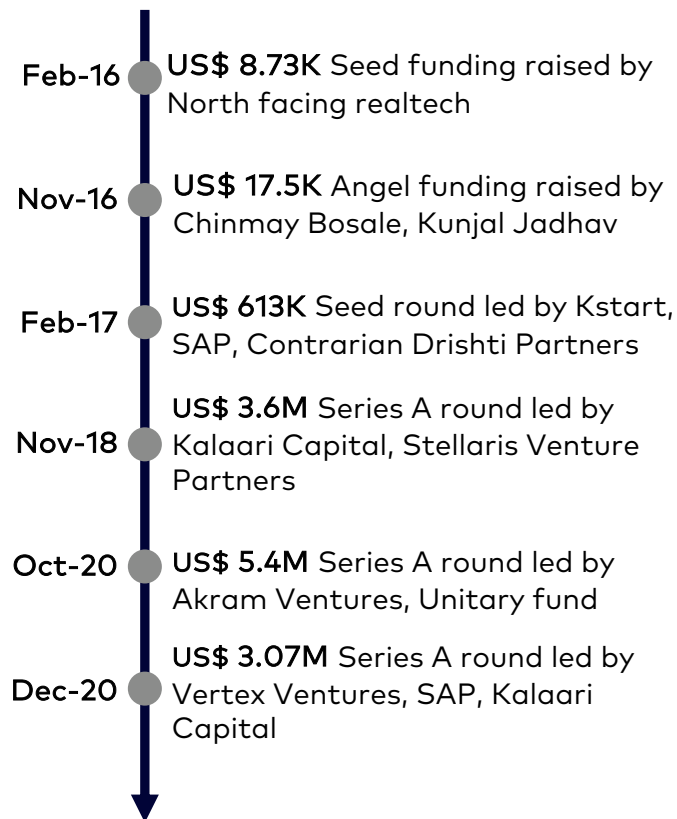


Total funding
US\$ 12.6M
(Series A)



Overview
Offers tools for customer verifications, employee verifications, user verifications, partner verification

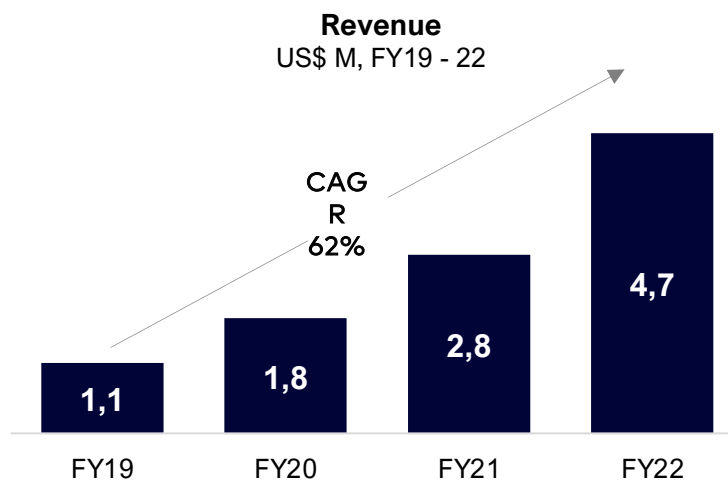
Funding timeline



Strengths

- Harnesses the latest technologies in AI to perform comprehensive identity verification using **liveliness checks, image forensics, face matching, and a randomized set of questions**
- Signzy video KYC solution has matured over **dialects, browsers and low-internet**

Financials



Type of solutions / technologies / services

Solution / service	Details
Video KYC	Liveliness check through assisted videos and face match selfies
Fraud checks	Multi-fraud control using 100s of data points including document forgery, mobile, email, IP validation
Fintech APIs	Comprehensive pre integrated API stack of over 240+ APIs across financial use cases
Deep user analytics	Getting deep insights into customer behavior by intelligent tracking of relevant current and historical data
Enterprise Grade security	Customers can manage their own data, privacy, security, storage and retrieval

Note(s): Information as of July 2022
Source(s): Industry reports, Company websites, Secondary research, Praxis analysis

Founded in 2014, HyperVerge offers ID verification, video KYC, face authentication and de-duplication in different industries



Founded
2014



Headquarters
Bangalore



150+
Employees



Total funding
US\$ 1M
(Seed)



Overview
A B2B SaaS company providing AI-based identity verification/ KYC solutions to enterprises in Fintech, Gaming, Crypto etc.

Product suite

Product	Details
IDV	<ul style="list-style-type: none"> Enables onboarding users instantly across the globe with high accuracy AI models for liveness detection, face-match & ID verification
Video KYC	<ul style="list-style-type: none"> Enables onboarding users remotely with very high confidence over video, with or without assistance from an agent
Face authentication	<ul style="list-style-type: none"> Enables authentication of repeat users & transactions instantly and helps deliver a better customer experience while preventing fraud
Face de-duplications	<ul style="list-style-type: none"> Fool-proof system to detect synthetic identity fraud in milliseconds

Marquee clients



Strengths

- Reduced customer drop-offs:** Helps reduce drop off rates to the tune of 50%
- Single image passive liveness technology:** Enables to convert more users by improving CX and verifying liveness with just a selfie and without any complex gestures or videos
- Seamless integration and fast deployment:** Integrating is a hassle-free activity with Web and Mobile SDKs with low-code workflow, saving developers' time and enables going live within hours

Value propositions

Value prop.	Details
Seamless customer onboarding	<ul style="list-style-type: none"> Reduce the time customers spend verifying their identities, reducing the drop-offs during the process
Increase approval rates	<ul style="list-style-type: none"> Better automated approval rates for identity checks to reduce the time and cost spent on manual verifications / reviews
Increased conversion	<ul style="list-style-type: none"> Streamline the onboarding process for a better customer experience and increased conversion
Agent Fraud Prevention	<ul style="list-style-type: none"> Protect the company's reputation by eliminating fraud & preventing fraudulent agents from entering the system
Face authentication	<ul style="list-style-type: none"> Verify agents and delivery executives in an instant using face authentication
Reward good users	<ul style="list-style-type: none"> Ensure good behaviour from users by identifying bad actors and rewarding good ones

Note(s): Information as of July 2022

Source(s): Industry reports, Company websites, Secondary research, Praxis analysis

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

FDP market landscape in Southeast Asia

FDP market landscape in Singapore

FDP market landscape in Indonesia

FDP market landscape in Malaysia

FDP market landscape in Vietnam

FDP market landscape in Thailand

FDP market landscape in Philippines

FDP playbook

Appendix

Internet users are expected to be 527M by 2027; digital transaction value was ~US\$ 186B in 2022 and is expected to be ~US\$ 379B by 2027

Smartphone users are expected to cross 526M by 2027, growing at a CAGR of 3%

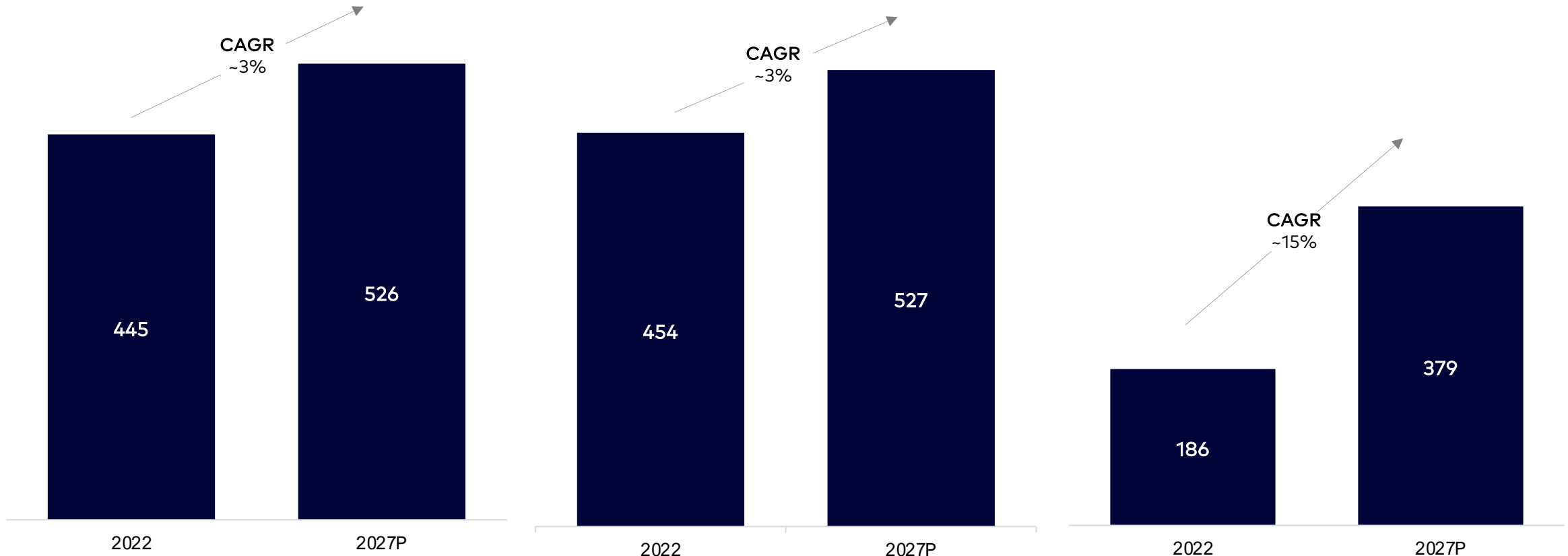
Internet users are expected to reach 527M by 2027, growing at a CAGR of 3%

Digital transactions value is expected to cross US\$ 350B by 2027

Smartphone users
In M, 2022 - 27P

Internet users
In M, 2022 - 27P

Value of digital transactions in
Fintech
In US\$ B, 2022 - 27P



Note(s): Only 6 countries are considered in the SEA region – Singapore, Indonesia, Malaysia, Thailand, Vietnam, Philippines
Source(s): Statista, Secondary research, Praxis analysis

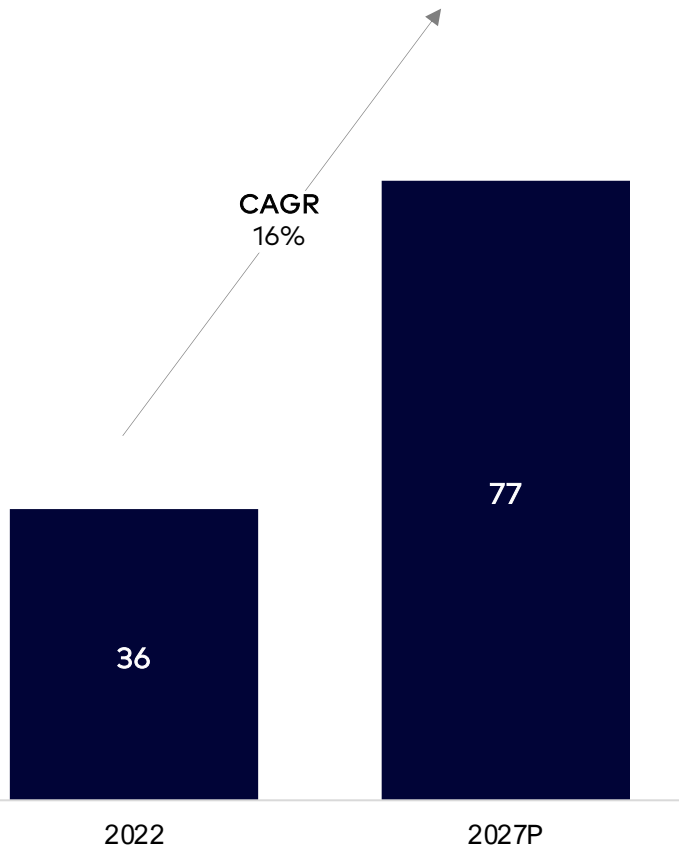
Of the total ~36B digital transactions witnessed in SEA region, 75%+ transactions are through mobiles; fraud attack rate is ~1.5%

Digital transactions volume in SEA is expected to reach 77B by 2027

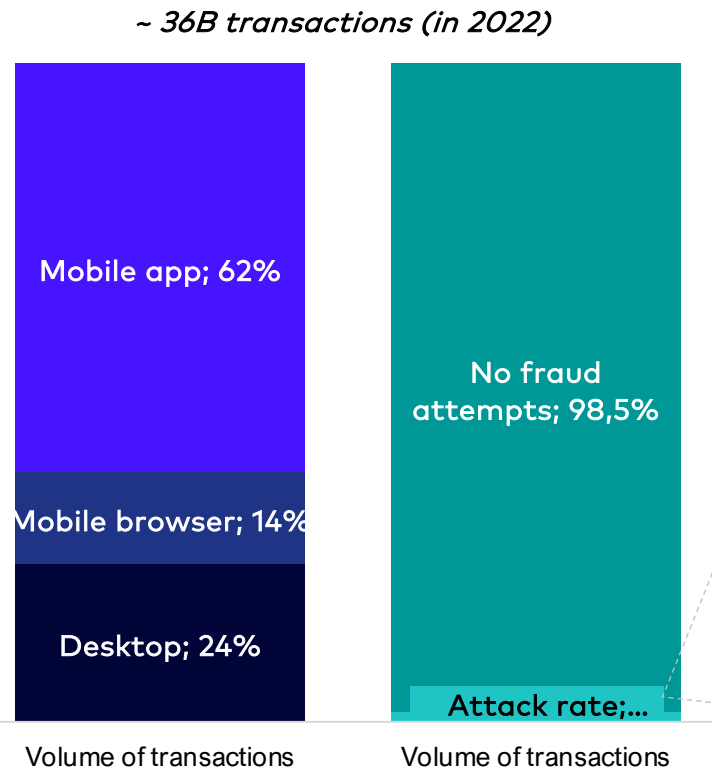
More than 75% transactions take place via mobiles; attack rate in SEA is ~1.5%

Even though majority of transactions are via mobile, ~58% fraud attacks are via desktop

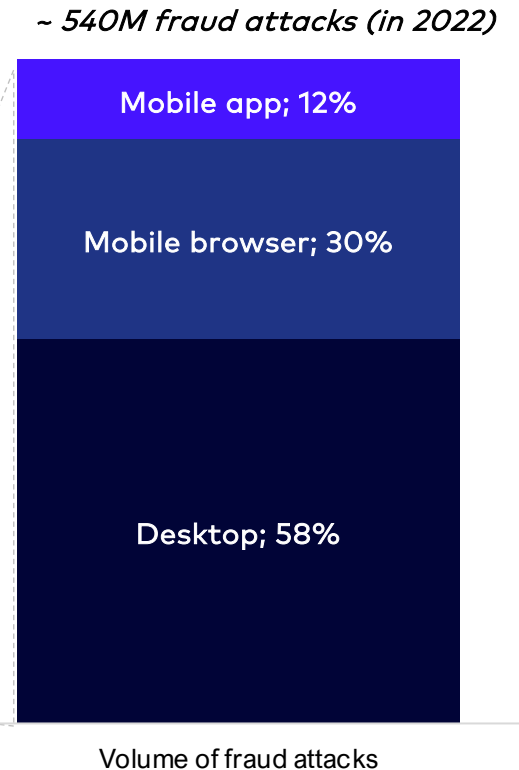
Volume of digital transactions
In B, 2022 - 27P



Transaction volume by channel and
attack rate
In %, 2022



Fraud volume split by channel type
In %, 2022



Note(s): Only 4 countries are considered in the SEA region – Singapore, Malaysia, Thailand and Philippines
Source(s): ACI Worldwide, GBG, LexisNexis global report, Secondary research, Praxis analysis

Synthetic identity, friendly fraud, and account takeover account for ~70% fraud losses across customer journey

Fraud costs are dominated by purchase transactions in financial services

Fraud costs are dominated by purchase transactions in e-commerce

Synthetic identity and friendly fraud losses constitute more than 55% of total losses

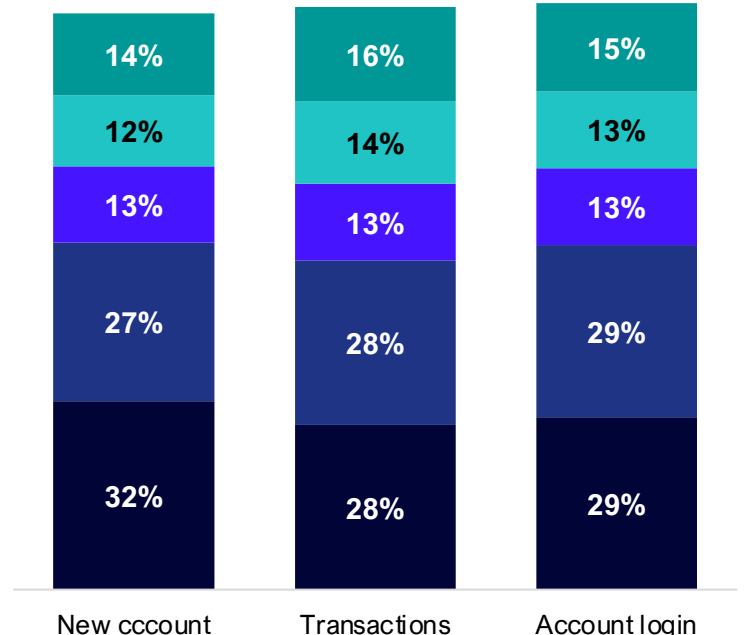
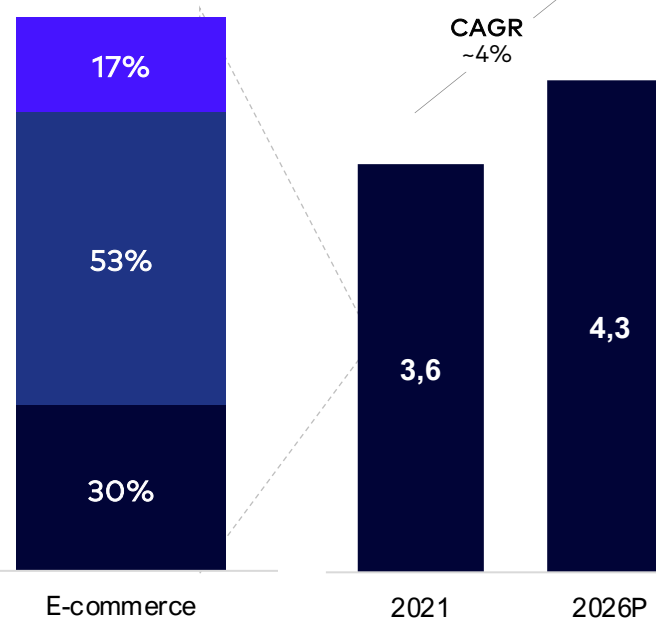
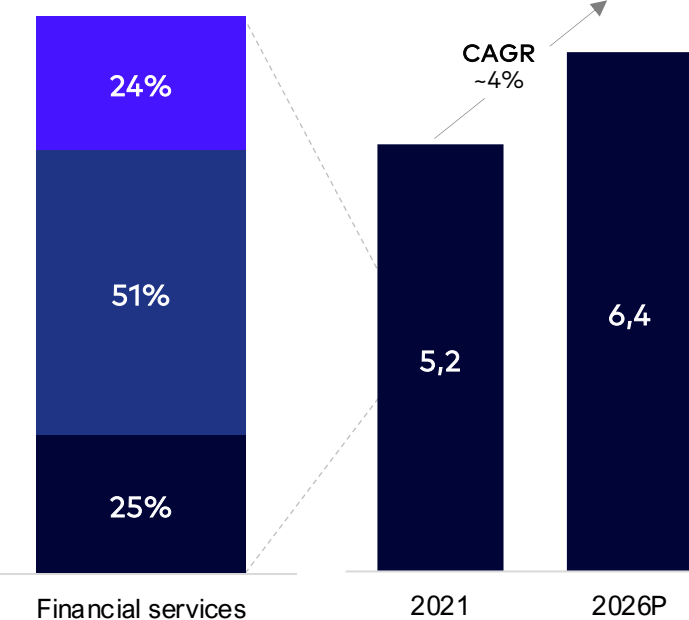
Fraud costs by customer journey stage
In %, 2022

Cost of fraud for unit dollar lost in transaction
In US\$, 2022-27P

Fraud costs by customer journey stage
In %, 2022

Cost of fraud for unit dollar lost in transaction
In US\$, 2022-27P

Distribution of losses by fraud type
In %, 2022
N = 387



- Account login
- Transactions
- New account creation

- Account login
- Transactions
- New account creation

- Lost / stolen merchandise
- 3rd party account takeover
- 3rd party / Synthetic identity fraud
- Fraudulent request for return / refund
- Friendly / 1st party fraud

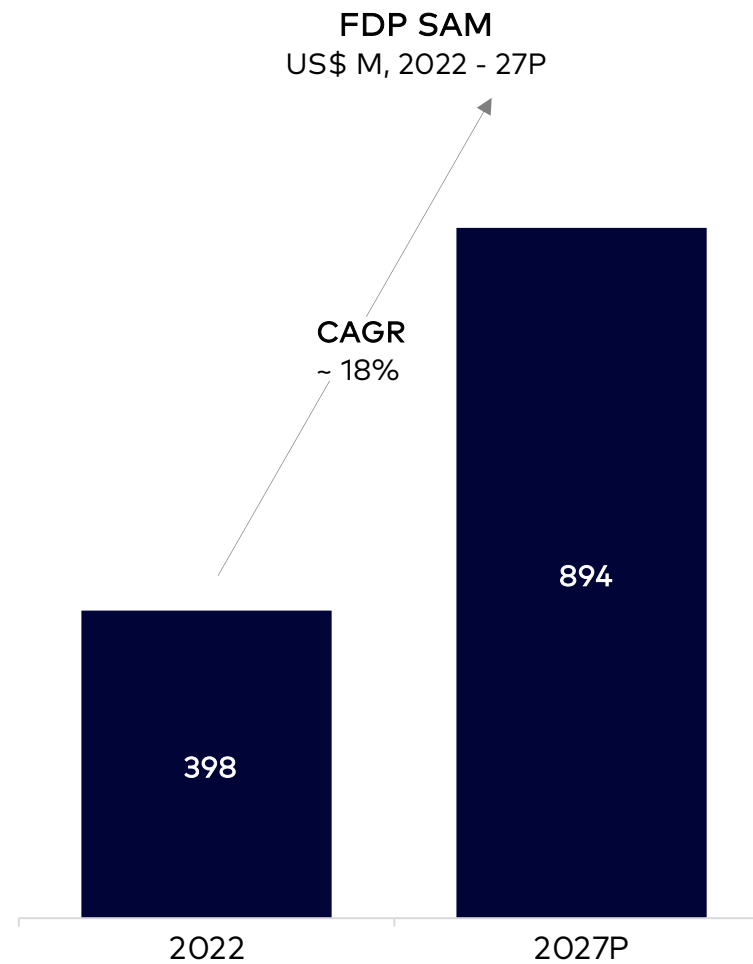
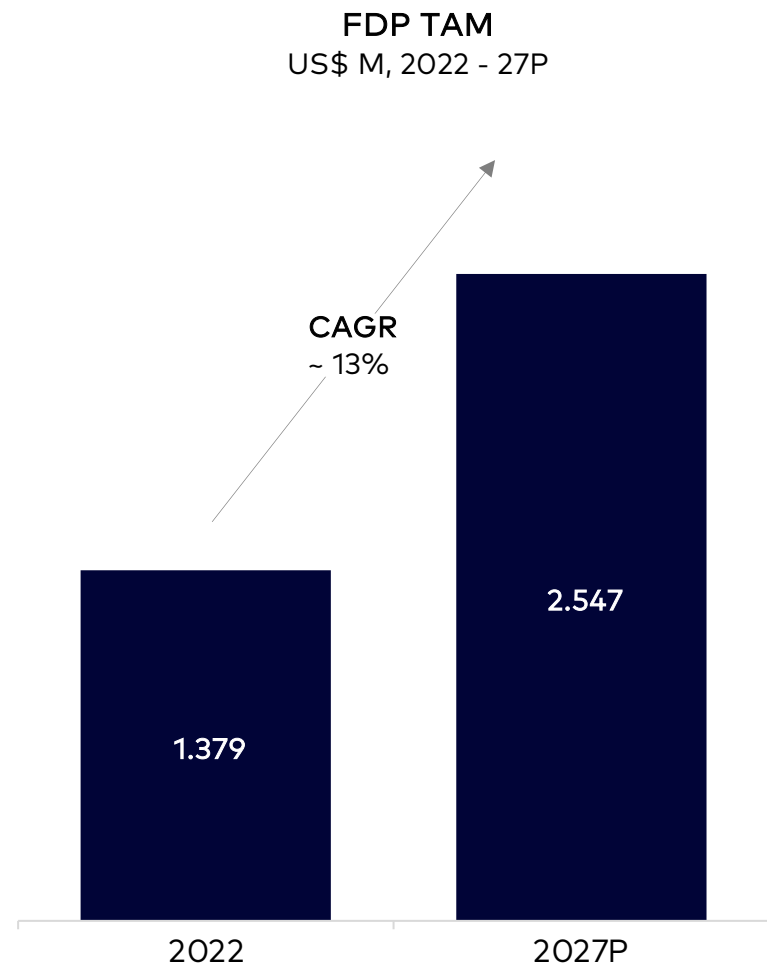
Note(s): Only 4 countries are considered in the SEA region – Singapore, Malaysia, Thailand and Philippines
 Source(s): Statista, LexisNexis industry report (Survey of N = 387 risk and fraud executives), Secondary research, Praxis analysis

Of the total US\$ 1,379M addressable FDP market, ~US\$ 398M is the serviceable addressable FDP market

FDP TAM was ~US\$ 1,379M in 2022 and is expected to be ~US\$ 2,547M in 2027

FDP SAM was ~US\$ 398M in 2022 and is expected to touch US\$ 900M in 2027

Rising online digital applications, shift to digital payments are the top growth drivers



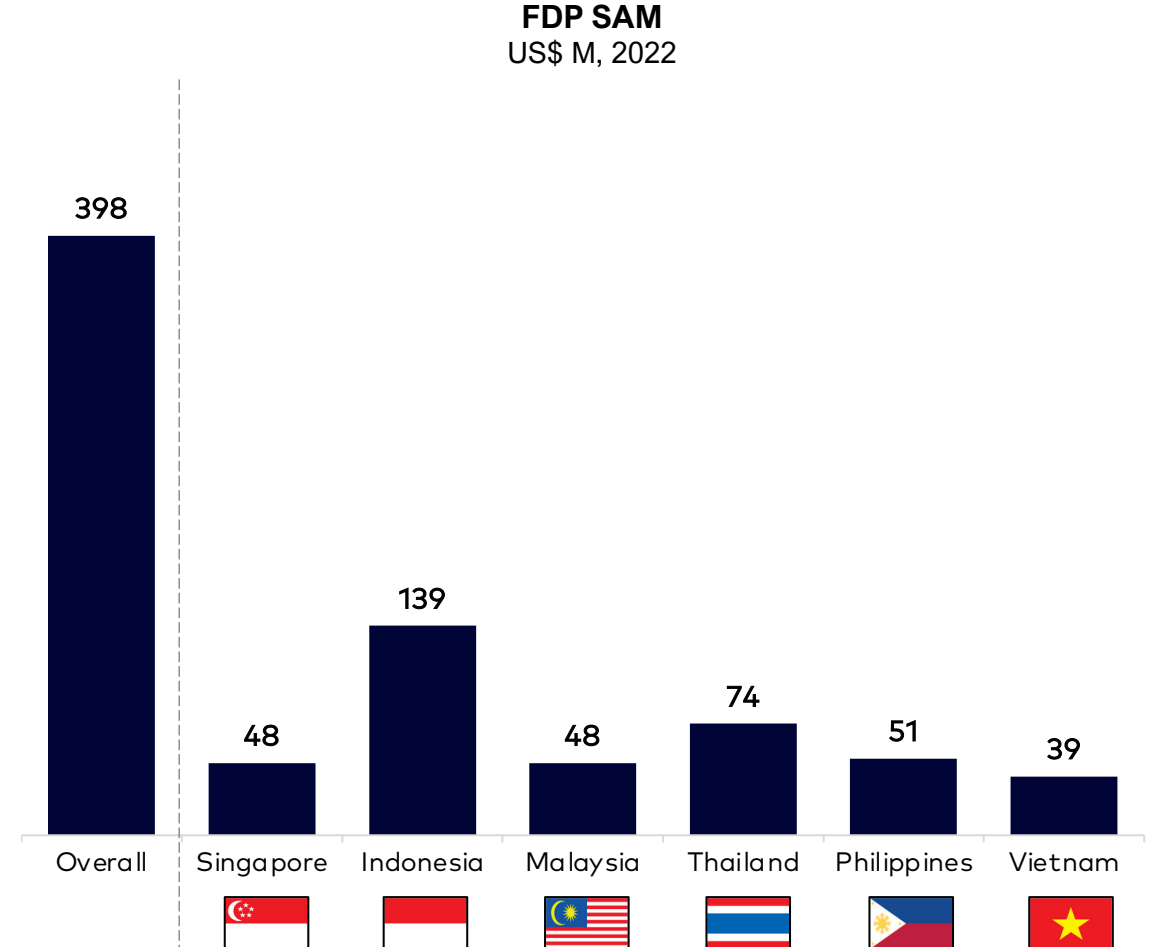
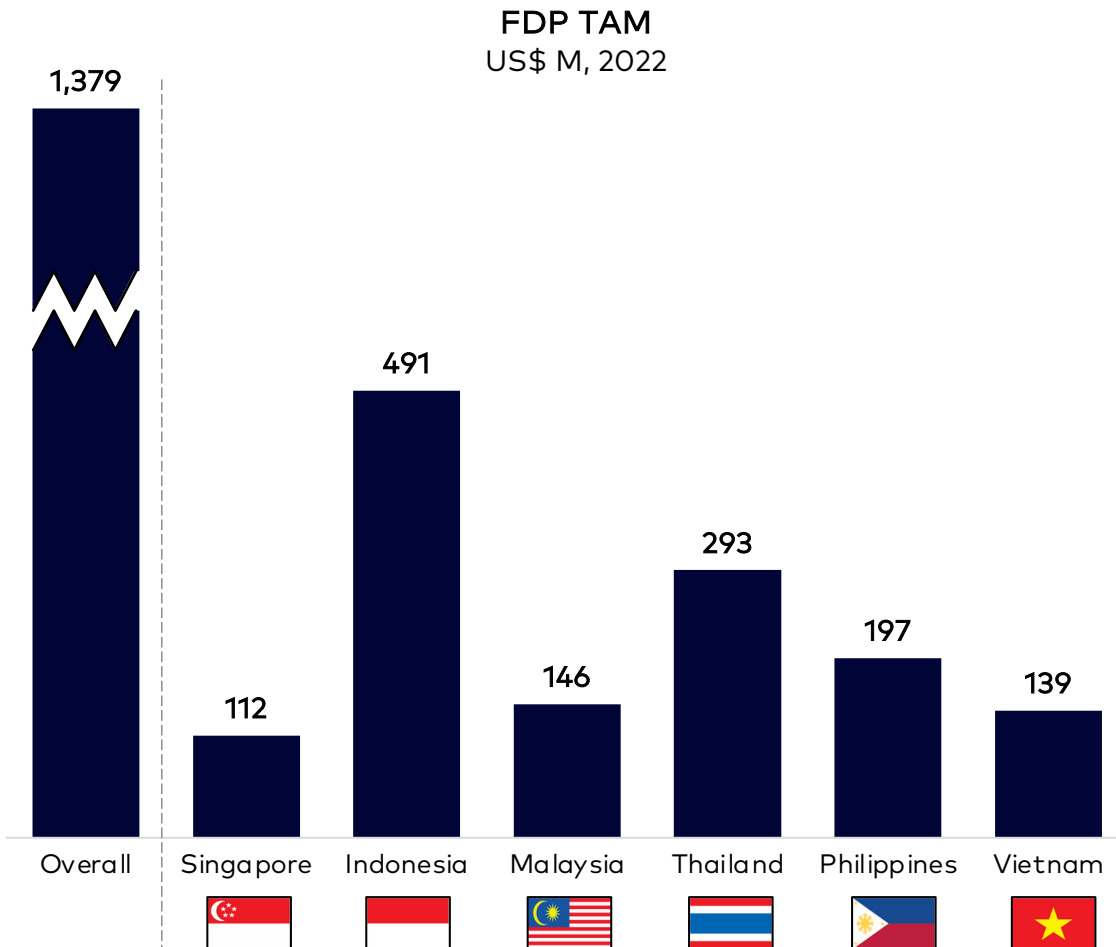
Growth factor	Details
Rise in online digital applications and services	<ul style="list-style-type: none"> Adoption of online digital applications are driving the growth for fake websites and mobile application
Adoption of digital payments and NFC technology	<ul style="list-style-type: none"> Digital payments and touchless financial transactions have also increased the points of vulnerabilities
Adoption of digitization and IoT	<ul style="list-style-type: none"> Connected devices collect, transmit, and store various consumer data creating privacy risks and giving access to fraud
Increasing sophistication of big data analytics	<ul style="list-style-type: none"> Big data analytics uses advanced analytics techniques like AI and ML, allowing organizations to proactively detect and prevent fraud across multiple digital channels

Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Among SEA countries, Indonesia has the maximum FDP TAM followed by Thailand

Indonesia (~US\$ 491M) held the largest share of total SEA FDP TAM followed by Thailand (~US\$ 293M) in 2022

Indonesia (~US\$ 139M) constituted ~35% of the total SEA FDP SAM in 2022



Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Fragmented data and inadequate data standardization are the main challenges whereas increased FDP investment and digitalization are the major opportunities

Opportunities / Tailwinds	Increase in investment budget for FDP	<ul style="list-style-type: none"> Organizations are looking at future-proofing fraud prevention through investment in fraud detection technologies As the number and maturity of FDP vendors increase, adoption of external services and products for fraud prevention is expected to increase, especially among the internet and digitally native companies
	Migration to digital solutions for onboarding and transaction monitoring	<ul style="list-style-type: none"> Banks and financial services companies have increased their use of internet and mobile apps for customer onboarding and unless advanced methods of fraud prevention are used, digital fraudsters can target inherent vulnerabilities using stolen ids, and device hacking A fraud is typically detected several weeks later, leading to significant increase in investigation efforts and time to recover lost money
	Increasing digitization	<ul style="list-style-type: none"> Digital payments in SEA stood at 36B in 2022, expected to reach 77B in 2027, growing at a CAGR of 16% Increased use of digital wallets, emergence of fintech apps and adoption of digital payments will require robust FDP solutions
	Increasing e-commerce growth	<ul style="list-style-type: none"> E-commerce growth rates in SEA countries is expected to be ~20%, which are largely led by verticalized and B2B ecommerce and D2C brands, those that do not have the required awareness, focus, technology infrastructure or spend capability on FDP
Challenges / Headwinds	Fragmented data	<ul style="list-style-type: none"> Large proportion of data resides in disparate legacy systems, increasing the number and cost of APIs required to collate and analyse data
	Lack of 360 degree customer view	<ul style="list-style-type: none"> A common challenge among organizations is not having a cohesive view of the customer journey through acquisition, onboarding, usage and transactions, which limits the analytical strength to proactively detect fraud and create the alert
	Unbanked population	<ul style="list-style-type: none"> Almost 50% of adults in Southeast Asia do not have access to any banking services, limiting the volume of digital transactions in the short term; however increasing digital penetration in the region is expected to significantly reduce this number in the medium to long term

Source(s): GBG and The Asia Banker (Survey of N=324 financial institutions), Primary conversations, Industry reports, Secondary research, Praxis analysis

The key purchase criteria for a FDP solution are the accuracy, pricing model, ability to handle a large volume of transaction, and ease of integration

<i>Most important</i>	Purchase criteria	Sub criteria	Customer rating	
	Features	<ul style="list-style-type: none"> • Fraud detection accuracy and false positive rate • Real-time tracking of transactions with automated decisions • Shortest response time • Customizability / configurability • Chargeback guarantee • End-to-end solutions or orchestration capability • Ability to handle the scale of transactions 	80 – 100%	<p>“Our primary aim was to decrease the false positives while not compromising on the fraud detection accuracy. We have successfully achieved this post the deployment of our current FDP solution”</p> <p>– <i>Product head, E-commerce</i></p>
	Cost	<ul style="list-style-type: none"> • Pricing model <ul style="list-style-type: none"> – Deployment cost – Monthly fees or subscription model – Micro fees based on API calls • Free trial and proof of concept 	70 – 100%	<p>“We needed custom FDP solutions specific to our existing model and use cases. We wanted the FDP solution to be well integrated with our model without hampering any ongoing operations / processes”</p> <p>– <i>Product manager, Insurance</i></p>
	User experience	<ul style="list-style-type: none"> • Ensuring customer education and awareness through meaningful SMS and emails sent at regular intervals to mitigate customer vulnerability 	50 – 75%	
	Integration and support	<ul style="list-style-type: none"> • Ease of integration of the FDP platform with existing tech tools • Support and training for smooth integration 	40 – 55%	<p>“Being one of the leading banks, we need a FDP solution which can manage a large transactional dataset in real-time with maximum possible accuracy”</p> <p>– <i>Fraud detection dept, Leading bank</i></p>
	Vendor reputation	<ul style="list-style-type: none"> • Reliability and credibility • Post-sale support • Reputation & customer reviews • Recommendation from peers 	40 – 50%	

Relatively less important

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

FDP market landscape in Southeast Asia

FDP market landscape in Singapore

FDP market landscape in Indonesia

FDP market landscape in Malaysia

FDP market landscape in Vietnam

FDP market landscape in Thailand

FDP market landscape in Philippines

FDP playbook

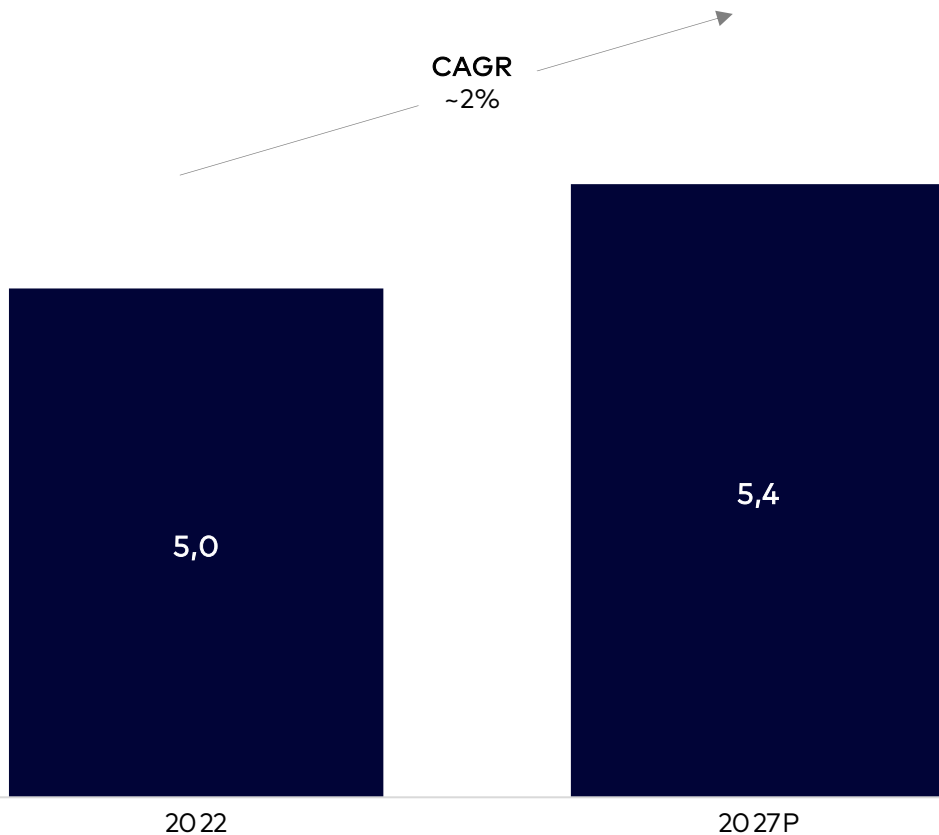
Appendix

Smartphone users and internet users are expected to reach ~5.4M and ~5.5M respectively by 2027

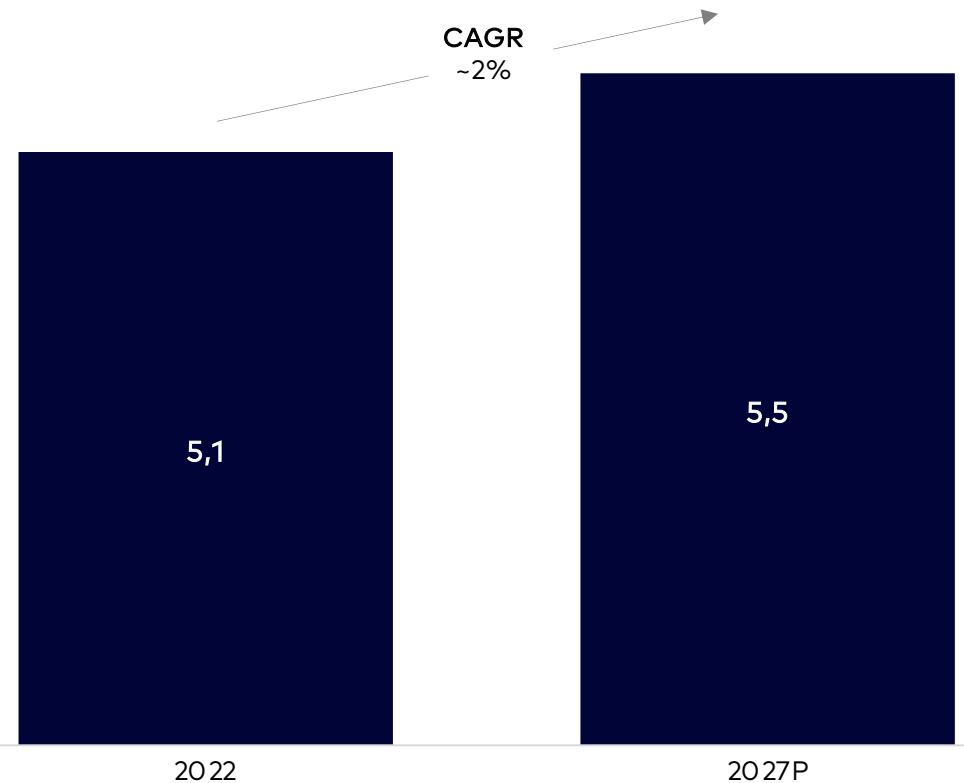
Smartphone users are expected to reach ~5.4M by 2027, growing at a CAGR of 2%

Internet users are expected to reach ~5.5M by 2027, growing at a CAGR of 2%

Smartphone users
In M, 2022 - 27P



Internet users
In M, 2022 - 27P



Source(s): Statista, World bank, Secondary research, Praxis analysis

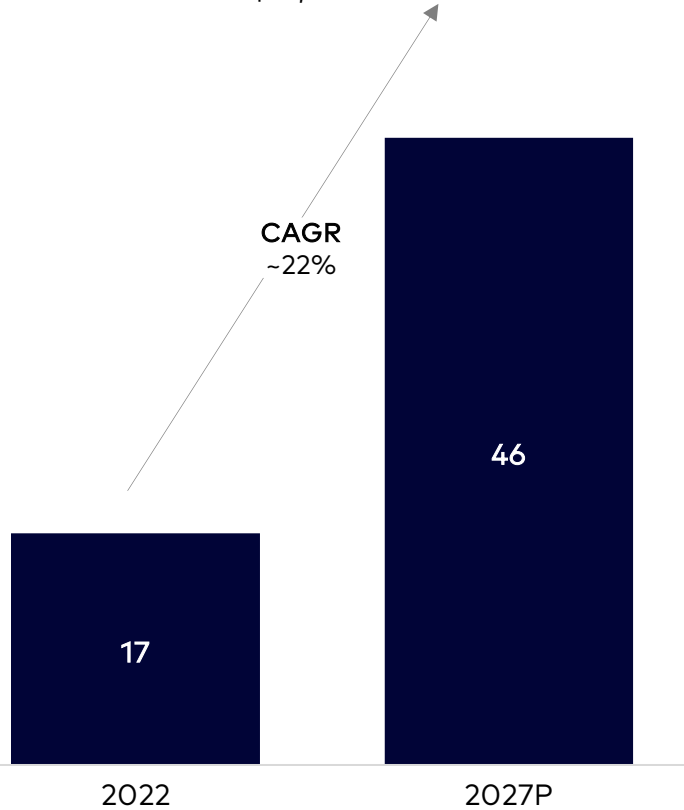
Digital transaction volume to reach ~3.1B by 2027; credit cards accounted for ~30% of the total digital transactions in 2021

Digital transactions value is expected to increase to ~US\$ 46B by 2027

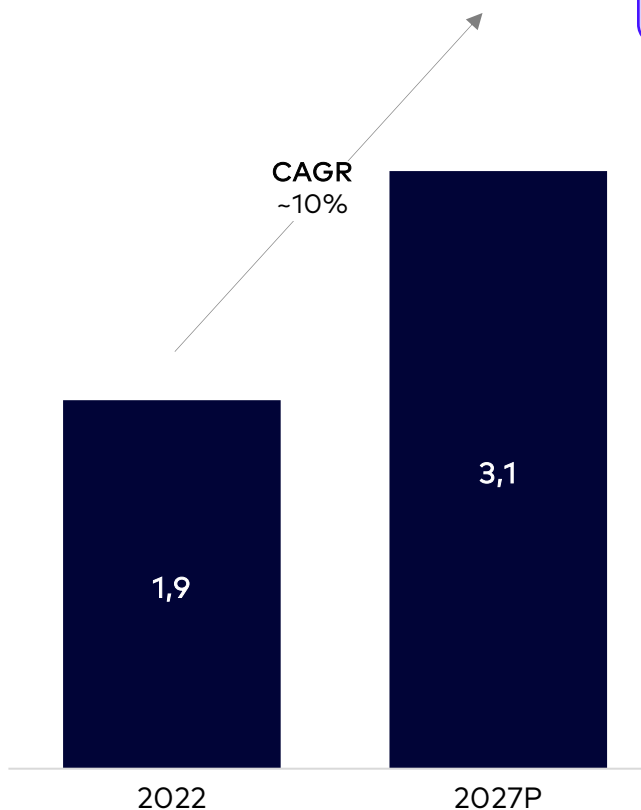
Digital transactions volume is expected to reach ~3.1B in 2027

More than 50% digital transactions happen through credit and debit cards collectively

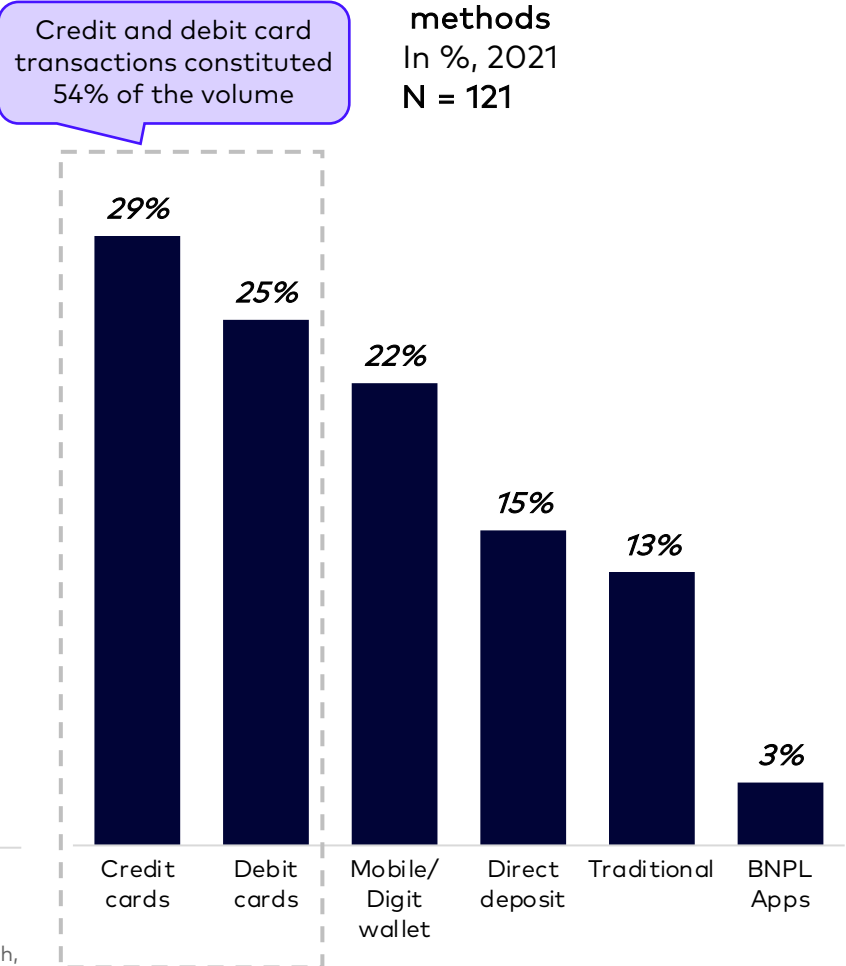
Value of digital transactions in Fintech
In US\$ B, 2022 - 27P



Volume of digital transactions
In B, 2022 - 27P



Transaction volume across payment methods



Source(s): Statista, ACI worldwide, LexisNexis industry report (survey of N = 121 fraud and risk executives across industries), Secondary research, Praxis analysis

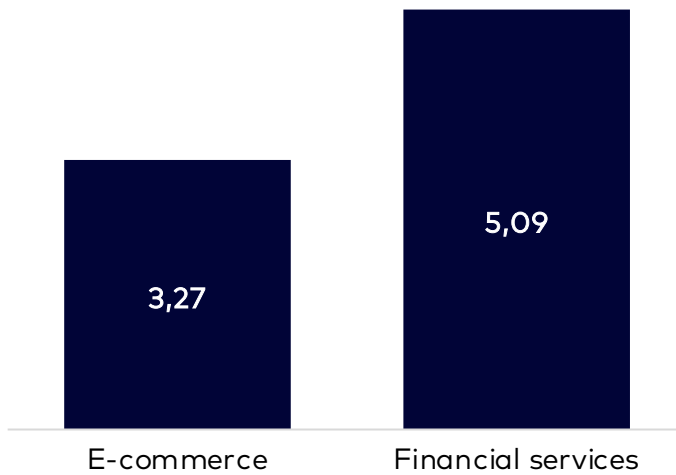
Fraud costs banks and financial services 5X the value of fraud which is largely contributed by transactions

Cost of fraud for unit amount lost in transaction is more than US\$ 5 in FS

Fraud costs across customer journey is dominated by purchase transactions

Synthetic identity and friendly fraud losses constitute more than 55% of total losses

Cost of fraud for unit amount lost in transaction
In US \$, 2021
N = 121

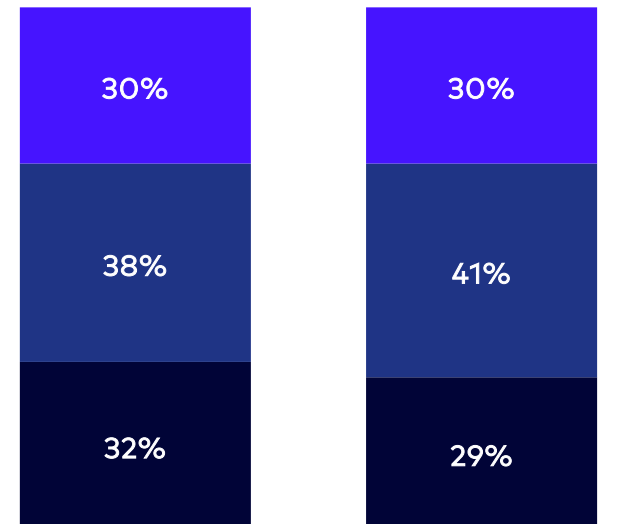


APAC avg. (US\$)

3.56

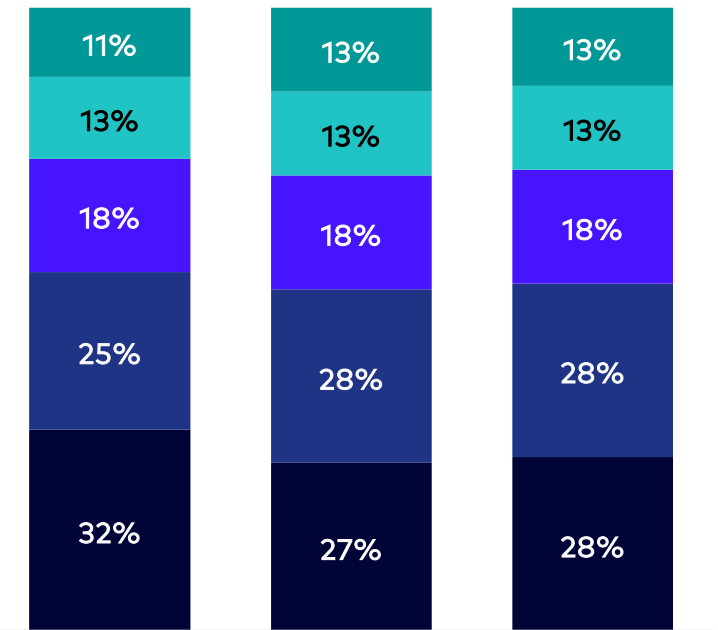
5.24

Fraud costs by customer journey stage
In %, 2021
N = 121



■ New account creation ■ Transactions ■ Account login

Distribution of losses by fraud type
In %, 2021
N = 121



■ Lost / stolen merchandise
■ Fraudulent request for return / refund
■ 3rd party account takeover
■ Friendly / 1st party fraud
■ 3rd party / Synthetic identity fraud

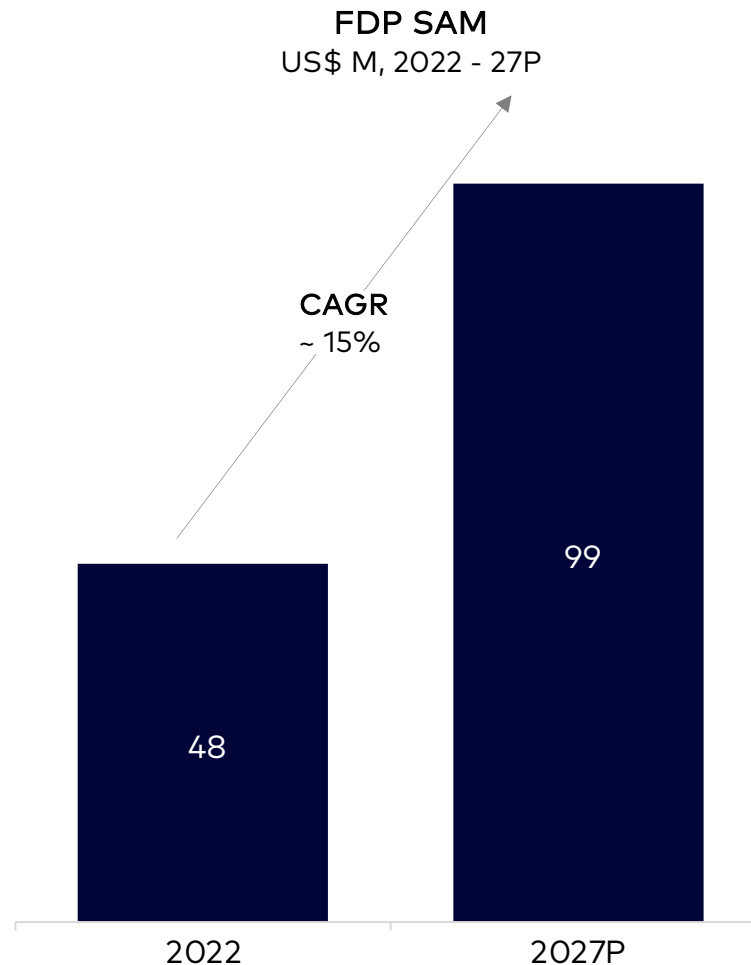
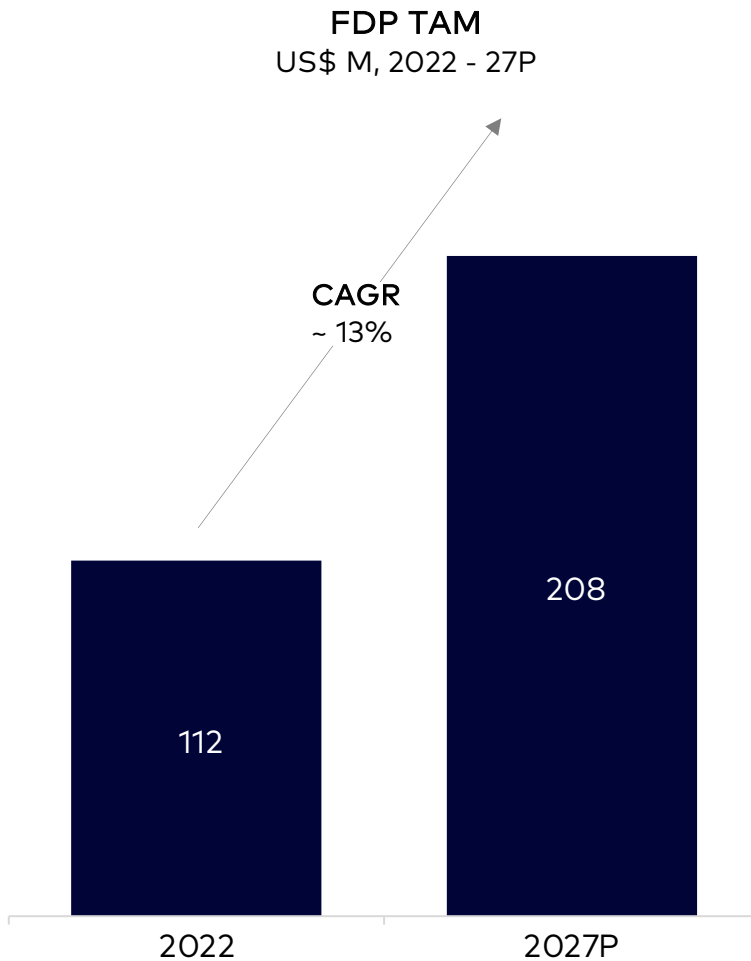
Source(s): Statista, LexisNexis industry report (survey of N = 121 fraud and risk executives across industries), Secondary research, Praxis analysis

Of the total US\$ 112M addressable FDP market, ~US\$ 48M was the serviceable addressable FDP market in 2022

FDP TAM was ~US\$ 112M in 2022 and is expected to be ~US\$ 208M in 2027

FDP SAM was ~US\$ 48M in 2022 and is expected to be ~US\$ 99M in 2027

High internet penetration, shift to digital channels are the top growth drivers



Growth factor	Details
High internet penetration	<ul style="list-style-type: none"> Internet penetration in Singapore is more than 90% resulting in higher volume of digital transactions across channels
Shift to digital channels	<ul style="list-style-type: none"> Pandemic has accelerated the adoption of digital banking and contactless payments → sharp increase in fraud attacks Digital payments volume is expected to cross 3B by 2027
Government regulations	<ul style="list-style-type: none"> The Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) is adopting measures to bolster the security of digital banking
Emergence of big data analytics	<ul style="list-style-type: none"> Big data analytics uses advanced analytics techniques like AI and ML, allowing organizations to prevent advanced fraud

Note(s): FDP TAM is the overall FDP market, whereas the FDP SAM includes the total outsourced market
 Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Digital transformation, increase in financial fraud are the drivers of FDP solutions adoption whereas limited data access is the main challenge

Opportunities / Tailwinds	Digital transformation	<ul style="list-style-type: none"> The digital transformation has led to an increase in account creations / contactless payments in Singapore, particularly among the e-Commerce merchants → greater potential for FDP players
	Increase in banking related fraud	<ul style="list-style-type: none"> Banking-related scams surged in the wake of the pandemic, leaving customers vulnerable to phishing and other means of fraud → need for FDP players to mitigate fraudulent activities
	Latency issues in banks	<ul style="list-style-type: none"> Due to latency issues, banks struggle in running deep-learning models at scale in real-time → a significant amount of fraud is going undetected
	Buy Now, Pay Later	<ul style="list-style-type: none"> The volume of transactions involving Buy Now, Pay Later apps and digital / mobile wallet providers is expected to continue to grow → increase in fraud attacks, and hence, the demand for FDP solutions
	Adoption of fraud management framework	<ul style="list-style-type: none"> Almost all digital banks and alternative finance providers including BNPL and digital wallets have not yet fully integrated cybersecurity and operations into fraud prevention processes
	Migration to digital solutions for onboarding and transaction monitoring	<ul style="list-style-type: none"> Banks and financial services companies have increased their use of internet and mobile apps for customer onboarding and unless advanced methods of fraud prevention are used, digital fraudsters can target inherent vulnerabilities using stolen ids, and device hacking Fraud are typically detected several weeks later, leading to significant increase in investigation efforts and time to recover lost money
Challenges / Headwinds	Limited access to third party data	<ul style="list-style-type: none"> Across both online and mobile channels, having limited access to real-time third-party data is a top factor in making customer identity verification a challenge for businesses in Singapore
	Increasing complexity of fraud attacks	<ul style="list-style-type: none"> While technology has eased fund transactions, it has also facilitated fraudsters in carrying out fraudulent transactions Fraudsters are constantly innovating new ways of infiltrating the financial systems with emerging advancements in technologies

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

FDP market landscape in Southeast Asia

FDP market landscape in Singapore

FDP market landscape in Indonesia

FDP market landscape in Malaysia

FDP market landscape in Vietnam

FDP market landscape in Thailand

FDP market landscape in Philippines

FDP playbook

Appendix

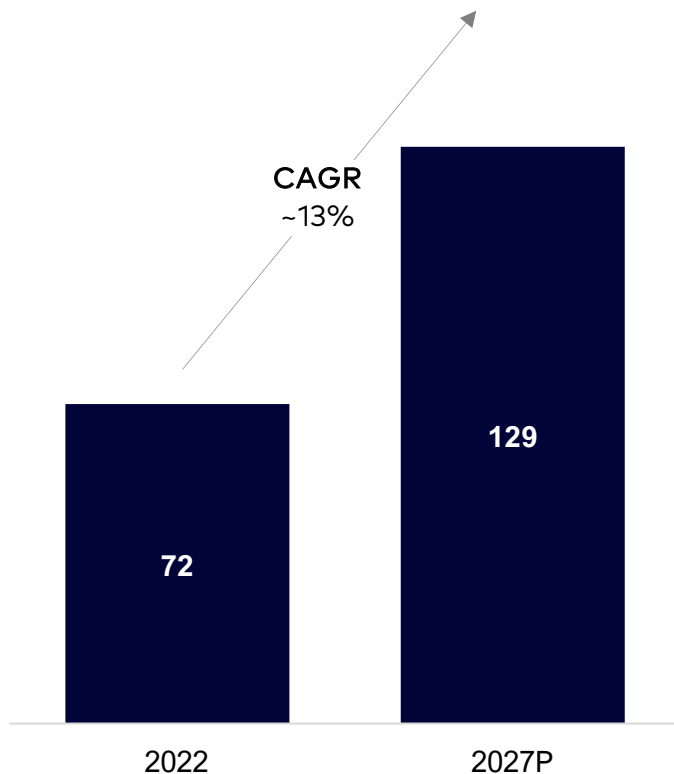
Driven by smart phone penetration and fintech advancement, digital transactions are expected to rise both in value and volume increasing the probability of fraud

Digital transactions value is expected to increase to ~ US\$ 129B by 2027

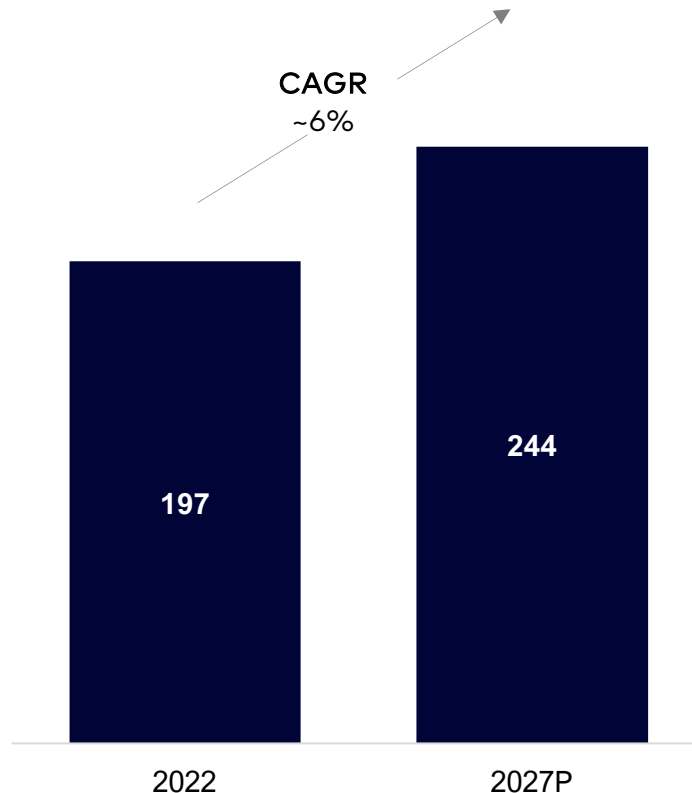
Mobile smart phone penetration to reach ~ US\$ 244M in 2027

Digital transactions volume is expected to grow at a CAGR of ~15%

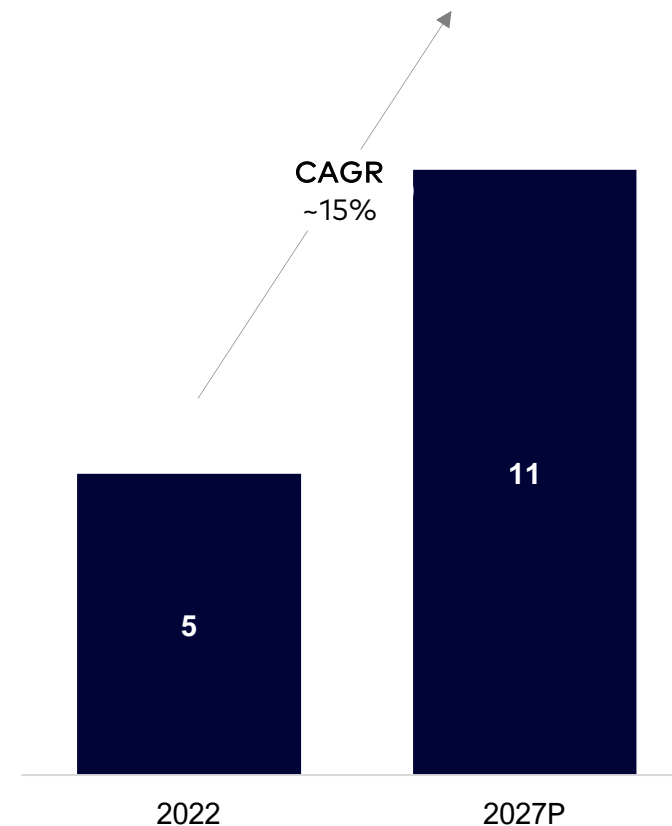
Value of digital transactions in Fintech
In US\$ B, 2022 - 27P



Mobile smart phone penetration
In M, 2022 - 27P



Volume of digital transactions
In B, 2022 - 27P

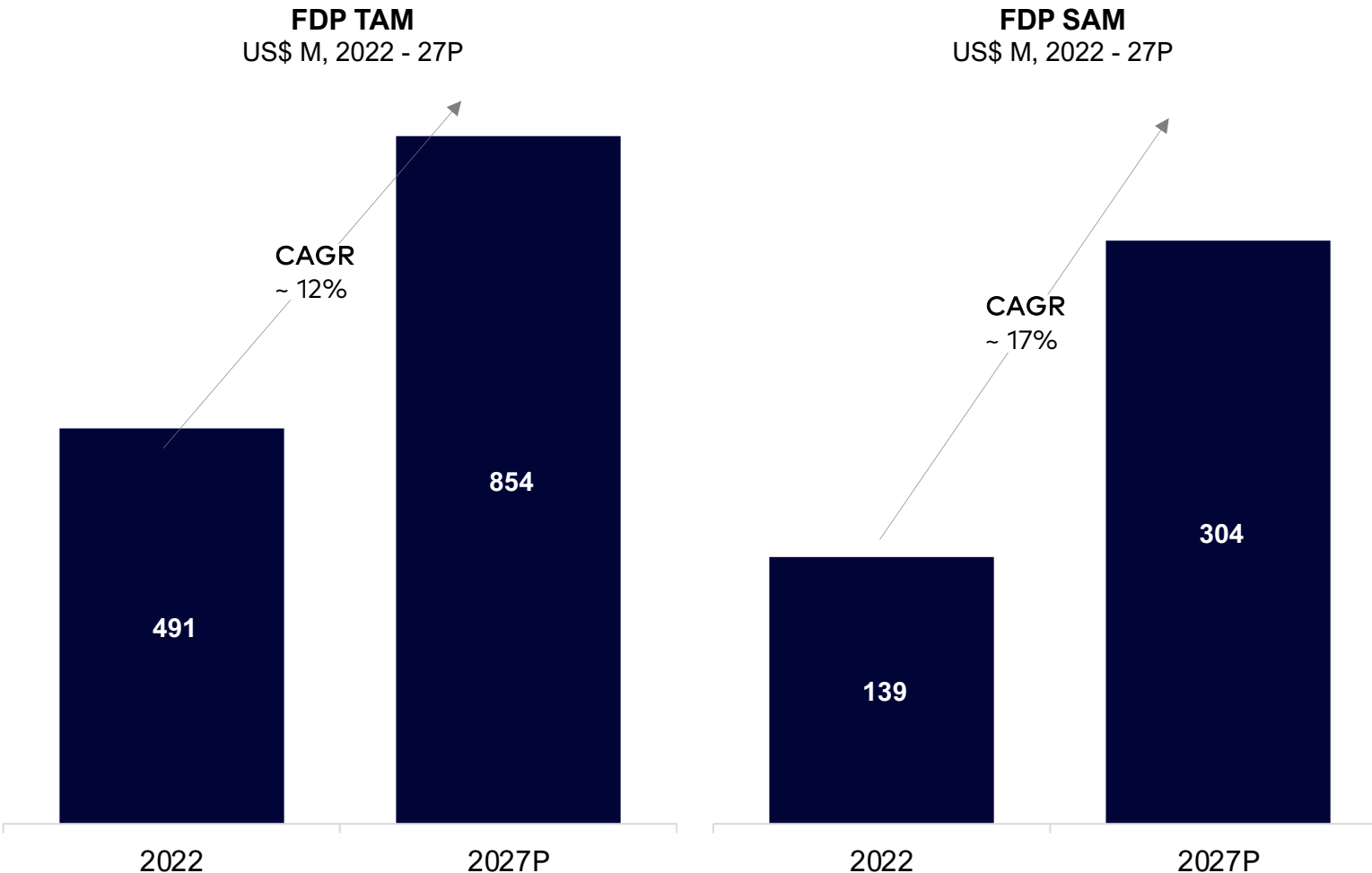


Of the total US\$ 491M addressable FDP market, ~US\$ 139M was the serviceable addressable FDP market in 2022

FDP TAM was ~US\$ 491M in 2022 and is expected to be ~US\$ 854M in 2027

FDP SAM was ~US\$ 139M in 2022 and is expected to be ~US\$ 304M in 2027

Rise in internet penetration, regulatory push by govt. are the top growth drivers



Growth factor	Details
Rise in internet penetration	<ul style="list-style-type: none"> There has been a significant growth in internet penetration from 34% in 2015 to 74% in 2022 resulting in higher volume of digital transactions
Regulatory push by govt	<ul style="list-style-type: none"> Indonesian govt has laid out specific laws to detect and prevent laws, promoting companies to have special Fraud Detection System (FDS) in place (Article 34)
Covid-19 impact	<ul style="list-style-type: none"> Pandemic pushed businesses to move online and provided people with the convenience of online platforms Even after the pandemic digital-first lifestyle didn't fade away fueling the growth of digital transactions
Shift to e-commerce	<ul style="list-style-type: none"> With more products being bought online, customers have changed their mode of purchase leading to increase in online transactions

Note(s): FDP TAM is the overall FDP market, whereas the FDP SAM includes the total outsourced market
 Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Inadequate data standardization is one of the main challenges whereas increased real-time payments and emergence of fintech start-ups are the major opportunities

Opportunities / Tailwinds	Growth in real-time payments	<ul style="list-style-type: none"> The outlook for real-time payments in Indonesia is excellent driven by their government’s clearly stated ambition to create an end-to-end integrated digital economy Real-time payments volume is projected to be 1.6B by 2026 which creates fraud vulnerabilities compelling organizations to adopt FDP solutions
	Emergence of fintech start-ups	<ul style="list-style-type: none"> 1100+ fintech startup companies have emerged in Indonesia out of which majority of them are payment service providers These companies are the largest adopters of FDP solutions implying greater opportunity for growth for FDP players in the Indonesian market
	Increase in investment budget for FDP	<ul style="list-style-type: none"> Organizations are looking at future-proofing fraud prevention through investment in fraud detection technologies FDP solution providers are getting room for growth because of these investments
Challenges / Headwinds	Fragmented data	<ul style="list-style-type: none"> The limitation resulting in ineffective fraud risk investigations is fragmented data as a result of piecemeal systems and software Large proportion of data resides in disparate legacy systems, increasing the number and cost of APIs required to collate and analyse data
	Inadequate data standardization	<ul style="list-style-type: none"> The lack of data standardisation and governance is a cause for ineffective fraud risk investigation Implementation becomes a challenge for FDP solution providers as client data is not standardised
	Lack of 360 degree customer view	<ul style="list-style-type: none"> A common challenge among organizations is not having a cohesive view of the customer journey through acquisition, onboarding, usage and transactions, which limits the analytical strength to proactively detect fraud and create the alert

Source(s): GBG and The Asia Banker (Survey of N=324 financial institutions), Secondary research, Praxis analysis

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

FDP market landscape in Southeast Asia

FDP market landscape in Singapore

FDP market landscape in Indonesia

FDP market landscape in Malaysia

FDP market landscape in Vietnam

FDP market landscape in Thailand

FDP market landscape in Philippines

FDP playbook

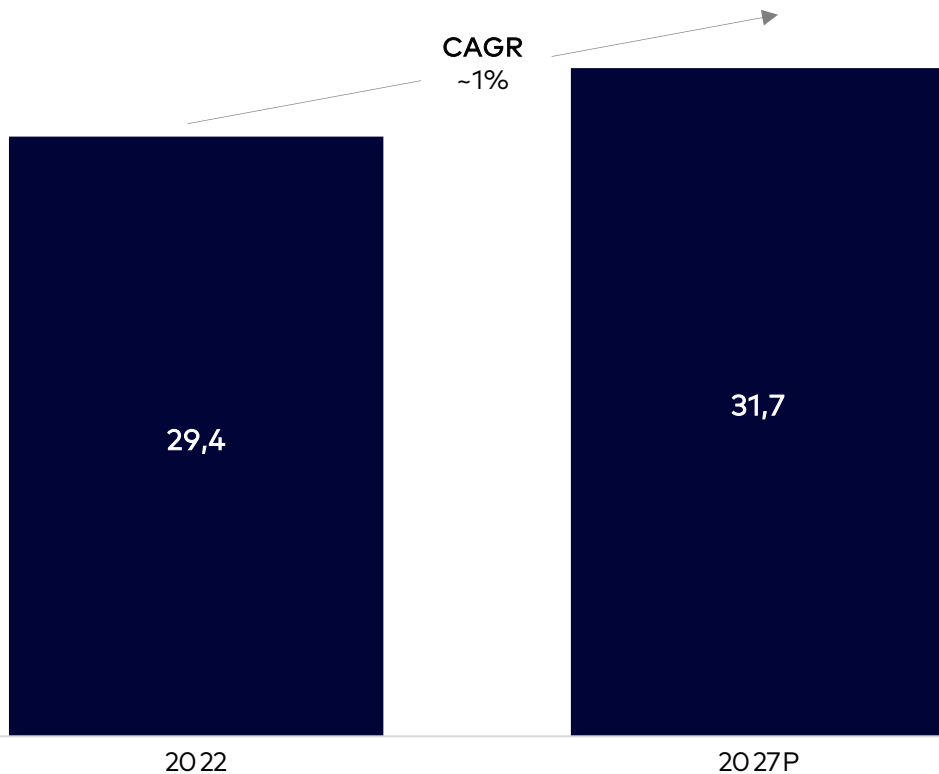
Appendix

Smartphone users and internet users were ~29.4M in 2022 and are expected to reach ~31.7M and ~31.6M respectively by 2027

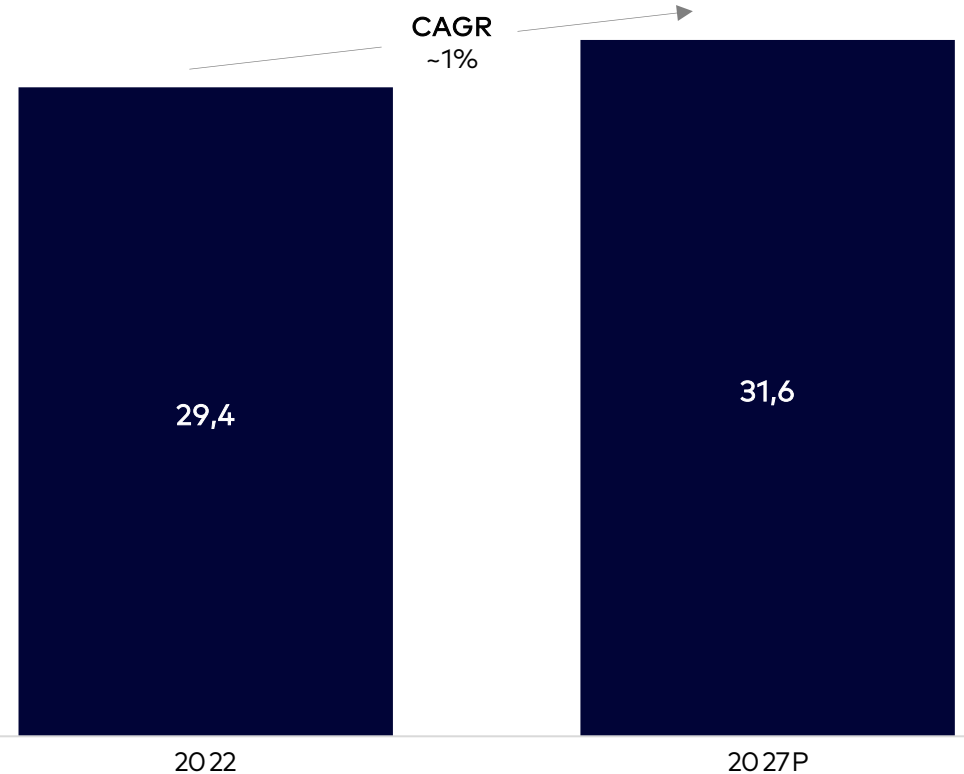
Smartphone users are expected to reach ~31.7M by 2027, growing at a CAGR of 1%

Internet users are expected to reach ~31.6M by 2027, growing at a CAGR of 1%

Smartphone users
In M, 2022 - 27P



Internet users
In M, 2022 - 27P



Source(s): Statista, World bank, Secondary research, Praxis analysis

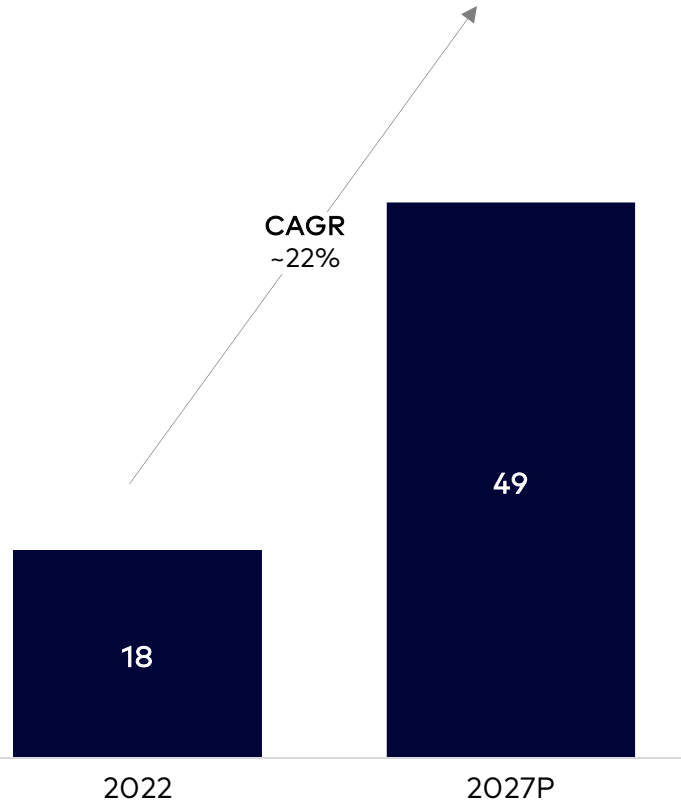
Digital transaction volume to reach ~17B by 2027; credit cards accounted for ~30% of the total digital transactions in 2021

Digital transactions value is expected to increase to ~US\$ 49B by 2027

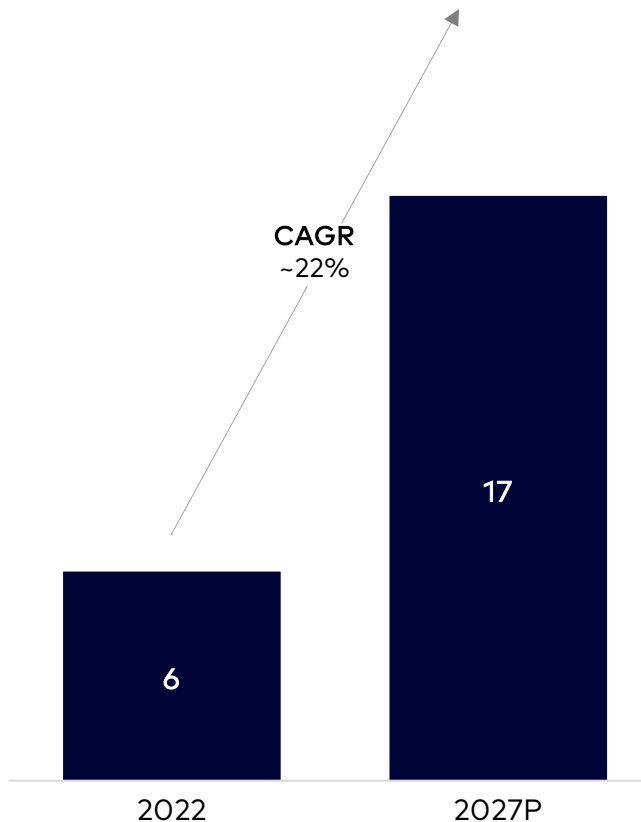
Digital transactions volume is expected to be ~16B in 2027, growing at ~22% CAGR

Most of the payments are made through credit and debit cards

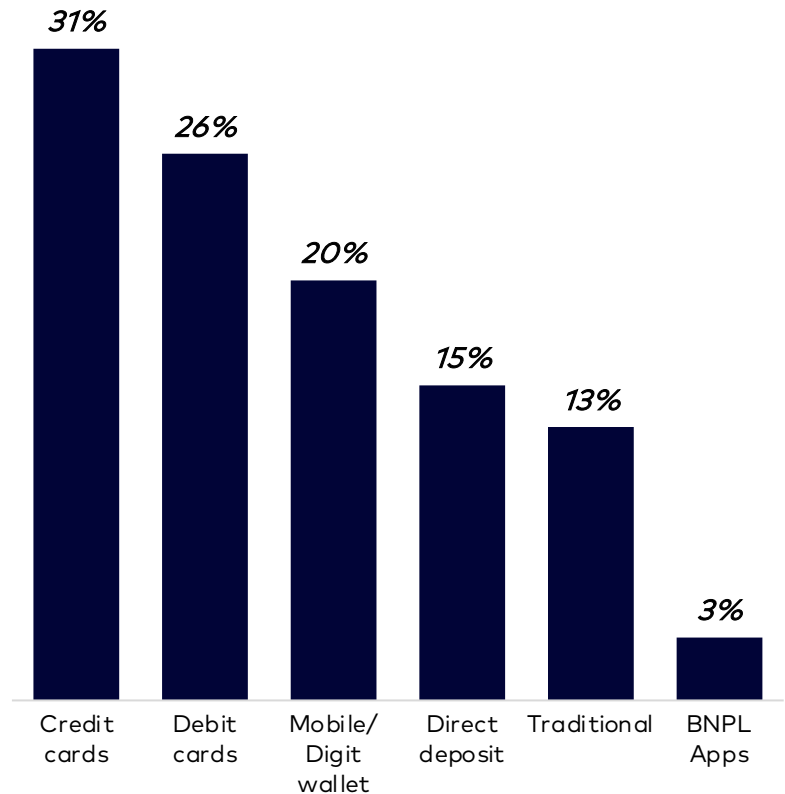
Value of digital transactions in Fintech
In US\$ B, 2022 - 27P



Volume of digital transactions
In B, 2022 - 27P



Transaction volume across payment methods
In %, 2021
N = 121



Source(s): Statista, ACI worldwide, LexisNexis industry report (survey of N = 121 fraud and risk executives across industries), Secondary research, Praxis analysis

Fraud costs banks and financial services 4.5X the value of fraud which is largely contributed by transactions

Cost of fraud for unit amount lost in transaction is more than US\$ 4.5 in FS

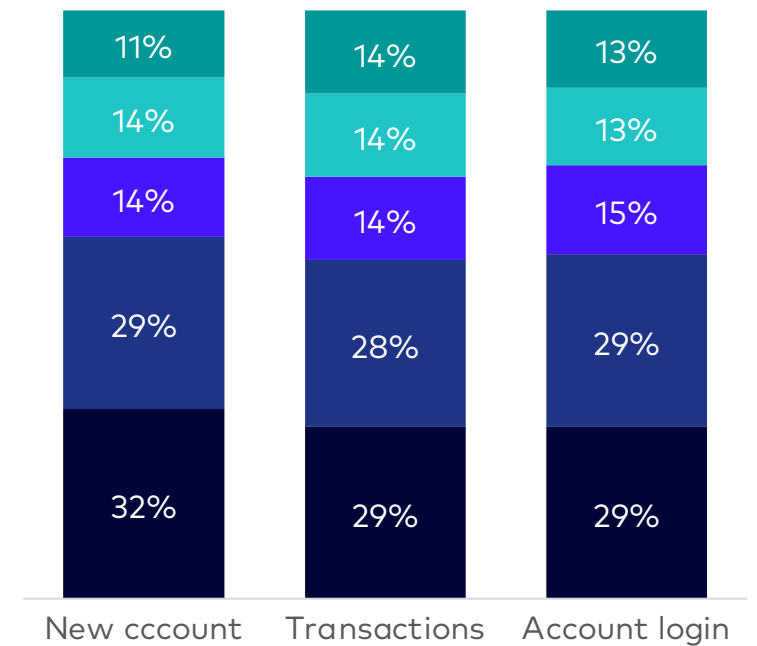
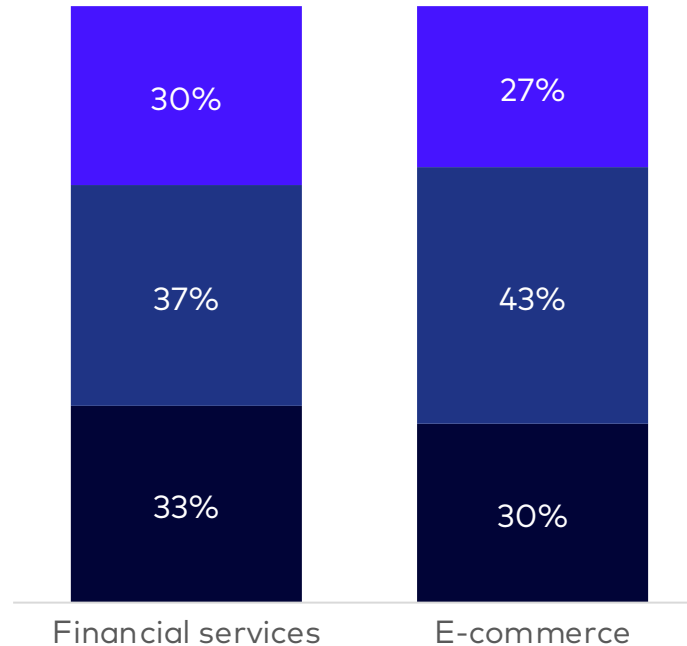
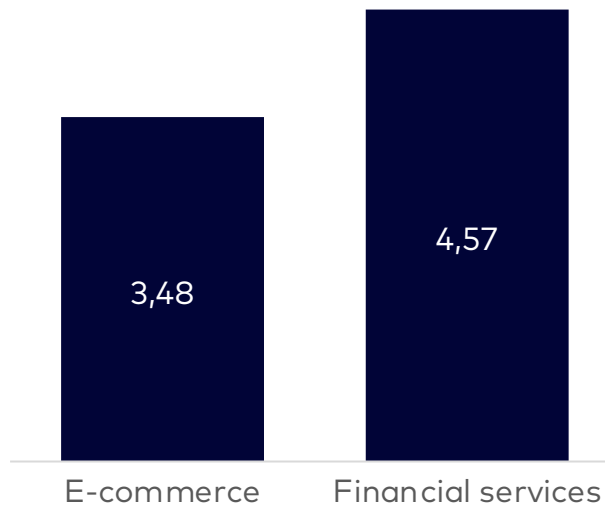
Fraud costs across customer journey is dominated by transactions

3rd party / Synthetic identity fraud constitute more than 30% of fraud losses

Cost of fraud for unit amount lost in transaction
In US\$, 2022
N = 121

Fraud costs by customer journey stage
In %, 2022
N = 121

Distribution of losses by fraud type
In %, 2021
N = 121



APAC avg. (US\$)

3.56

5.24

■ New account creation ■ Transactions ■ Account login creation

■ Lost / stolen merchandise
■ Fraudulent request for return / refund
■ 3rd party account takeover

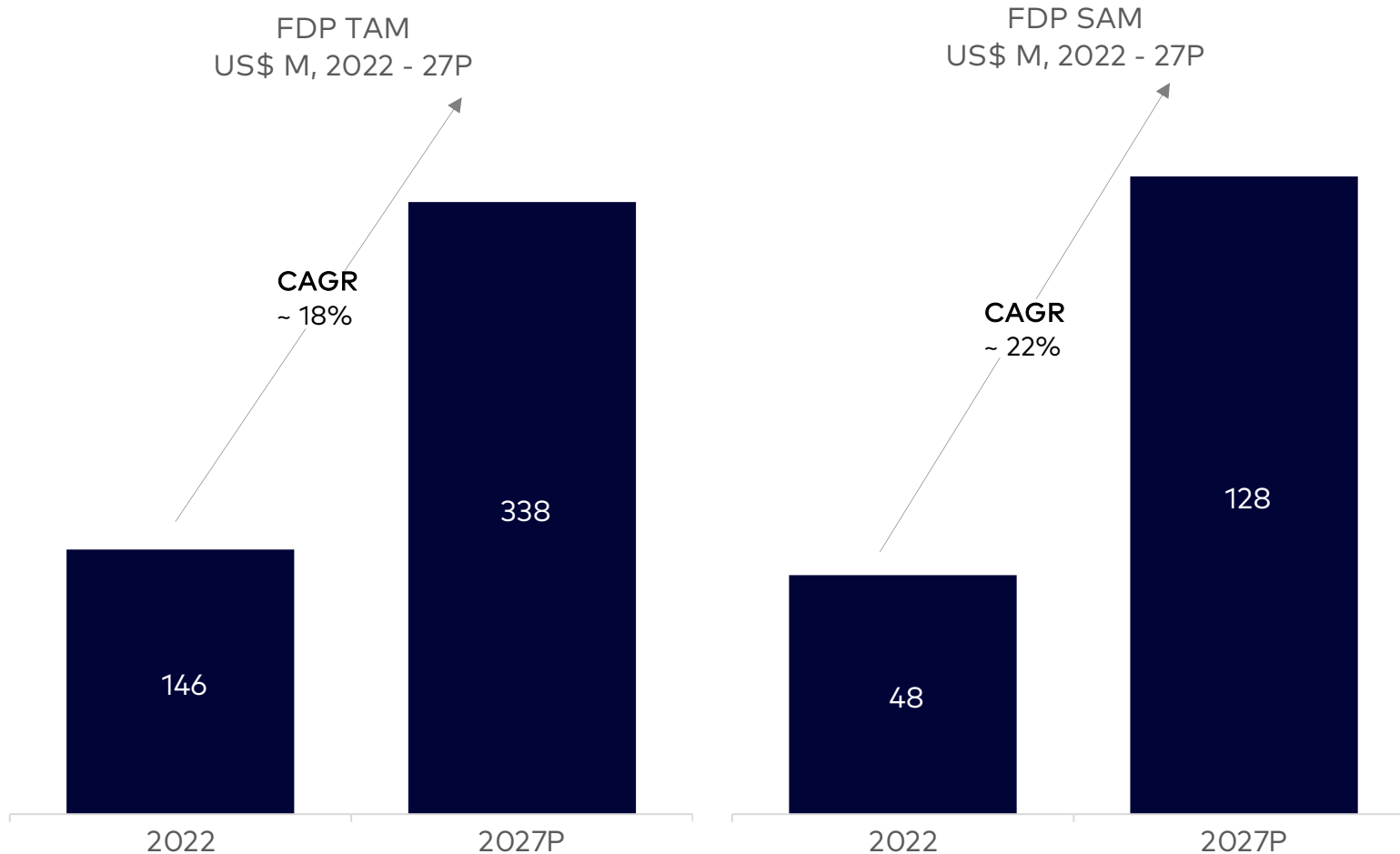
Source(s): Statista, LexisNexis industry report (survey of N = 121 fraud and risk executives across industries), Secondary research, Praxis analysis

Of the total US\$ 146M addressable FDP market in Malaysia, ~US\$ 48M was the serviceable addressable FDP market in 2022

FDP TAM was ~US\$ 146M in 2022 and is expected to be ~US\$ 338M in 2027

FDP SAM was ~US\$ 48M in 2022 and is expected to be ~US\$ 128M in 2027

Regulators intervention, rise in internet penetration are the top growth drivers



Growth factor	Details
Increasing focus from regulators	<ul style="list-style-type: none"> Bank Negara Malaysia (BNM) updated its Risk Management in Technology (RMiT) policy to include need for automated fraud detection system to monitor all financial transactions by leveraging heuristic behavioural analysis
Increasing internet penetration	<ul style="list-style-type: none"> At 89%, the high internet penetration in 2022, will drive the adoption of internet related services and eventually FDP solutions
Increased digitization	<ul style="list-style-type: none"> With increased digitization and the changing economic environment, more number fraud are expected in the next few years
Adoption of digital payments and NFC technology	<ul style="list-style-type: none"> Volume of digital payments are expected to grow at 22% between 2022 - 27 Touchless financial transactions have further increased the points of vulnerabilities for a potential fraud attack

Note(s): FDP TAM is the overall FDP market, whereas the FDP SAM includes the total outsourced market
 Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Digital transformation will foster the adoption of FDP solutions whereas conservative budget for fraud and risk management act as a deterrent

Opportunities / Tailwinds	Digital transformation of Malaysian businesses	<ul style="list-style-type: none"> • Significant increase in remote channel use, digital payment methods and omnichannel among Malaysian businesses • Rapid growth in use of mobile channels for payment like digital wallets (increased use of e-wallets like Boost, GrabPay etc.) and ordering via Buy Online/ Pick Up in Store (BOPIS) and curbside pickup becoming commonplace in the midst of the pandemic
	Likely increased use of third-party FDP solutions	<ul style="list-style-type: none"> • Malaysian firms are more likely to use third-party solutions to combat digital fraud and manual review rates, average time for order reviews, and order approval rates to measure their fraud prevention performance
	Preference for end-to-end fraud management platform	<ul style="list-style-type: none"> • End-to-end fraud management platform readiness is a key differentiation to driving digital product preference for 56% of Malaysian financial institutions
Challenges / Headwinds	Conservative budget for FDP solutions	<ul style="list-style-type: none"> • Malaysia had the most conservative estimated fraud risk and management technologies budget of US\$ 74 M per company • On average, the estimated budget to purchase new fraud prevention technology in APAC in 2020-21 is at US\$ 83 M
	Lack of real-time data availability	<ul style="list-style-type: none"> • More real-time third-party data is needed to help firms better balance speed of approval against customer abandonment before transaction completion
	Increasing complexity of fraud attacks	<ul style="list-style-type: none"> • Fraud attacks are becoming more sophisticated and this is an increasing challenge among many businesses in Malaysia • Fraud attacks like sophisticated bot attacks, social engineering fraud etc are growing in number, and making it difficult to detect and prevent fraud

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

FDP market landscape in Southeast Asia

FDP market landscape in Singapore

FDP market landscape in Indonesia

FDP market landscape in Malaysia

FDP market landscape in Vietnam

FDP market landscape in Thailand

FDP market landscape in Philippines

FDP playbook

Appendix

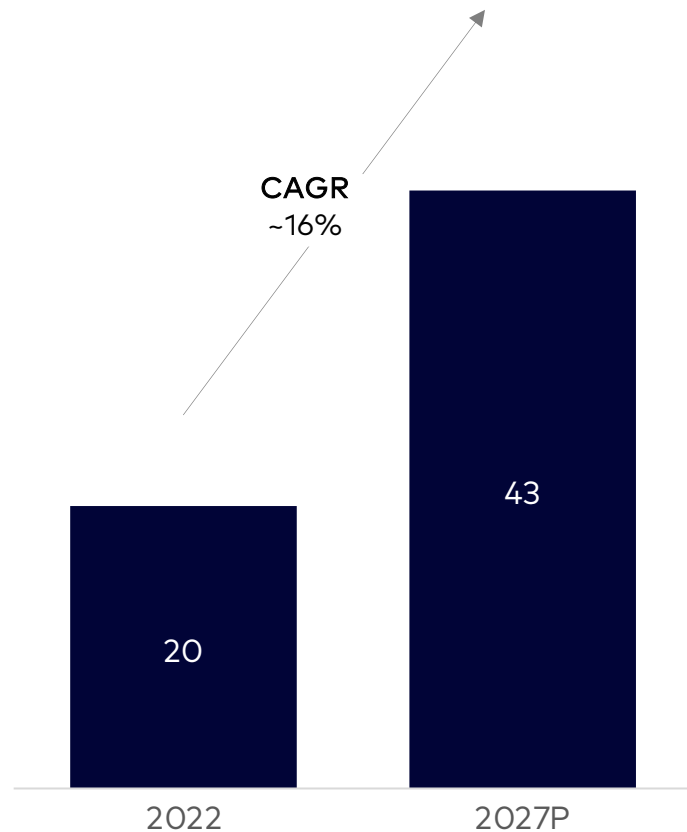
Value of digital transactions is expected to grow at ~16%; Digital transactions volume is expected to grow at ~12% between 2022 - 27

Digital transactions value is expected to increase to ~US\$ 43B by 2027

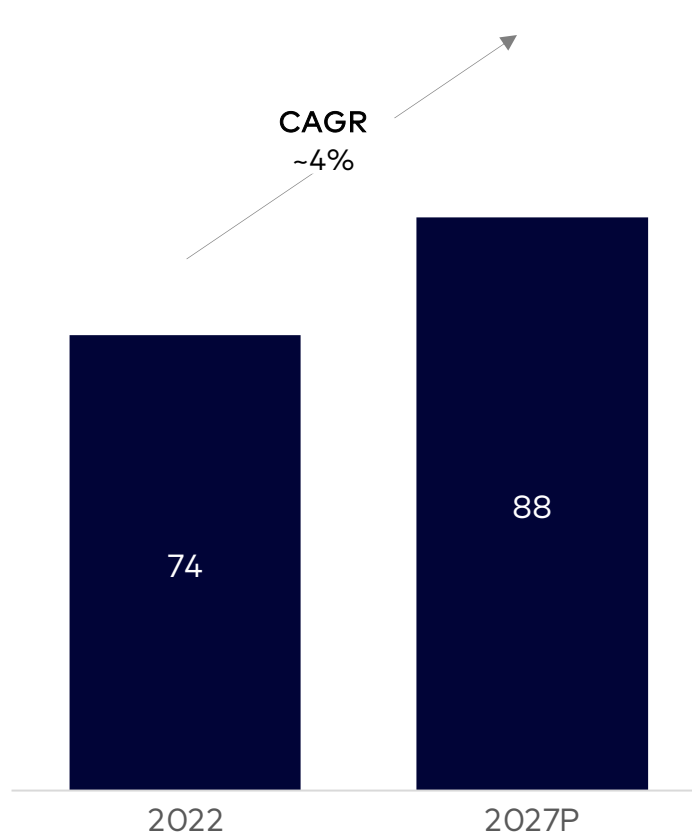
Mobile smartphones penetration to reach 88M in 2027

Volume of digital transactions expected to grow at a CAGR of ~12%

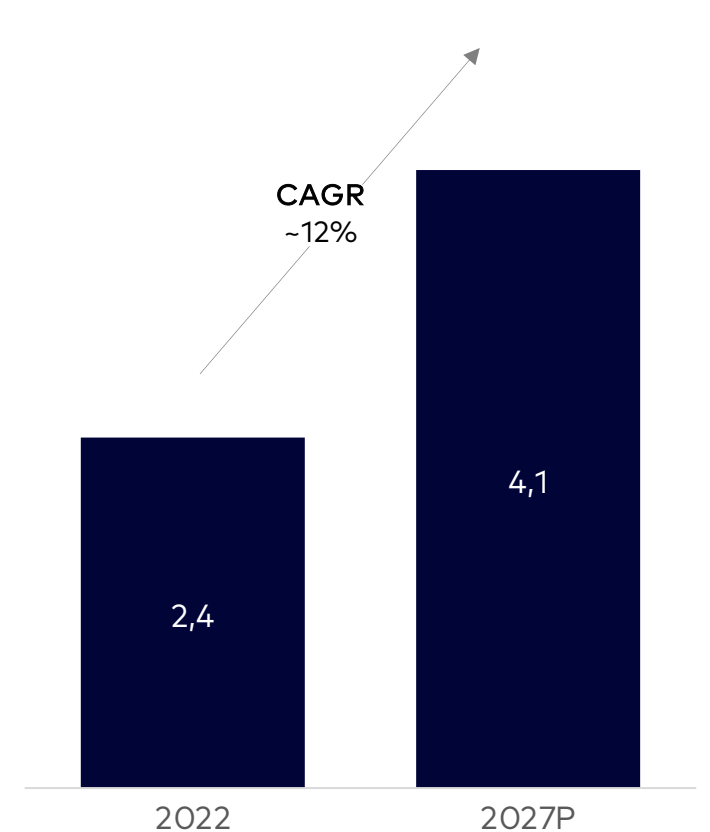
Value of digital transactions in Fintech
In US\$ B, 2022 - 27P



Mobile smart phone penetration
In M, 2022 - 27P



Volume of digital transactions
In B, 2022 - 27P



Source(s): Statista, ACI worldwide, GBG, Secondary research, Praxis analysis

Of the total US\$ 139M addressable FDP market in Vietnam, ~ US\$ 39M was the serviceable addressable FDP market in 2022

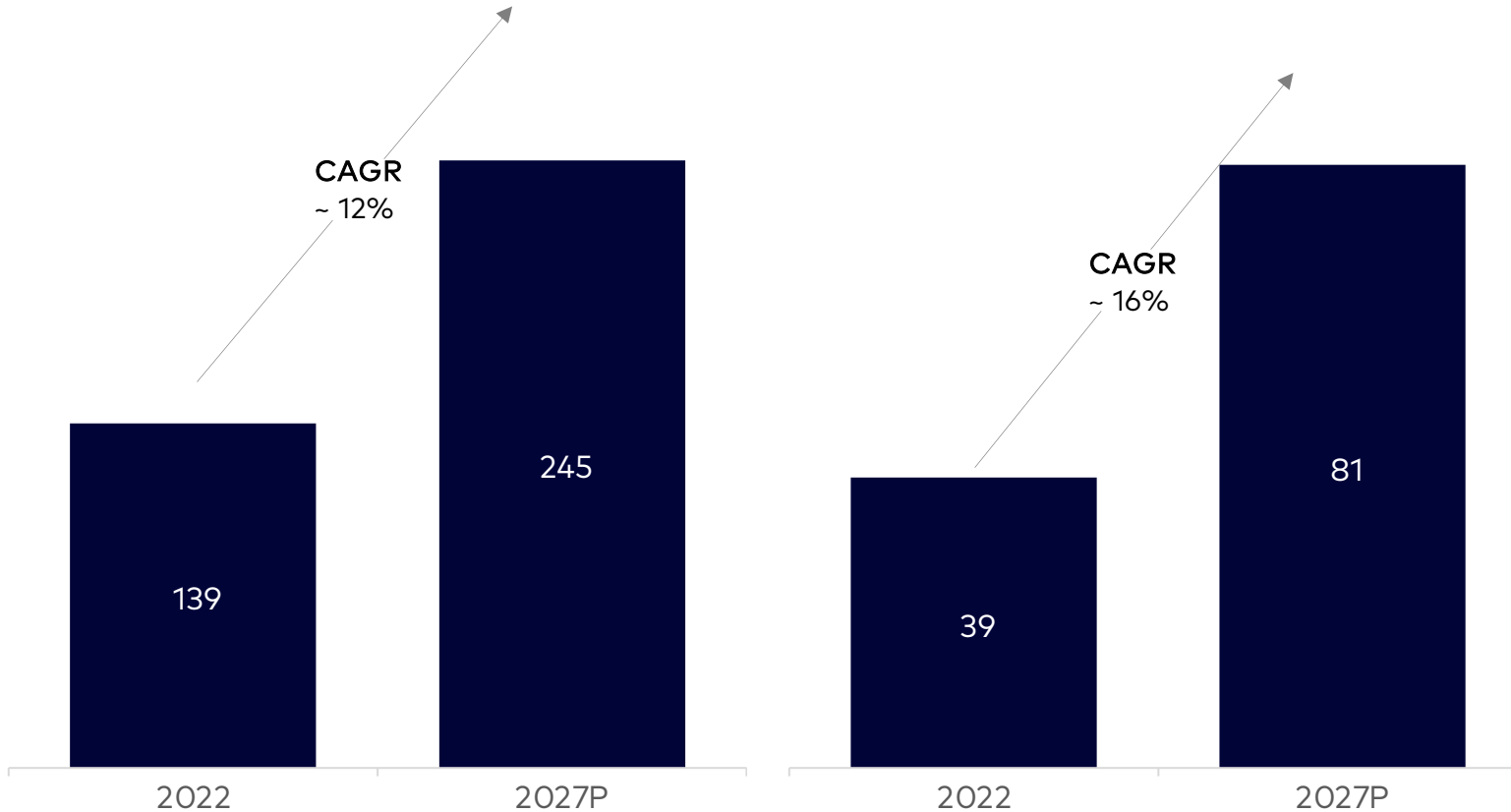
FDP TAM was ~US\$ 139M in 2022 and is expected to be ~US\$ 245M in 2027

FDP SAM was ~US\$ 39M in 2022 and is expected to be ~US\$ 81M in 2027

High fraud rate & regulatory push by the govt will drive the adoption of FDP solutions

FDP TAM
US\$ M, 2022 - 27P

FDP SAM
US\$ M, 2022 - 27P



Growth factor	Details
High & growing internet penetration	<ul style="list-style-type: none"> Internet penetration in Vietnam currently is ~ 73% and growing at 3.4%, to will lead to an increased focus on fraud detection and prevention
Highest fraud rate in SEA	<ul style="list-style-type: none"> Vietnam's fraud rate is the highest in SEA at 59.2% With anti-fraud measures slower to develop than the economy, fraudsters are seeing this emerging market as a perfect target; to drive adoption of FDP solutions in the coming years
Regulatory push by Vietnam Govt	<ul style="list-style-type: none"> Vietnamese govt introduced laws which have greatly focused on decreasing fraud rates As an example, cybersecurity law is aimed at tracking down traces and collecting evidence of online fraudulent appropriation of assets.
Rise in online digital applications & transactions	<ul style="list-style-type: none"> Adoption of online digital applications are driving the growth for fake websites and mobile application Increasing digital transactions (at a CAGR of 12%) are leading several digital companies to adopt FDP solutions and technologies to mitigate growing avenues of fraud

Note(s): FDP TAM is the overall FDP market, whereas the FDP SAM includes the total outsourced market
Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Rising adoption of digital payments and a very high fraud rate in the country will push companies to focus on fraud detection and prevention solutions

Opportunities / Tailwinds	Increasing adoption of digital payments	<ul style="list-style-type: none"> Volume of mobile payment transactions in Vietnam are expected to grow by 50-80%, number of internet payments to increase by 35%-40% annually, and the rate of individuals and organisations using cashless payments to reach 40% Creates a possible opportunity for FDP market with increasing digital transactions
	Preference for end-to-end fraud management platform	<ul style="list-style-type: none"> Preference for end-to-end fraud management platform is a key differentiation to driving digital product preference for 56% of Malaysian financial institutions
	AI / ML adoption	<ul style="list-style-type: none"> Adoption of AI / ML and other advanced technologies in anomaly and fraud detection in e-commerce firms has aided the FDP market to become more accurate This will enable faster, more efficient and accurate fraud detection and prevention by companies
	Highest fraud rate in SEA	<ul style="list-style-type: none"> Vietnam's fraud rate is the highest in SEA -> more than 50% companies have experienced a fraud in the last 2 years With anti-fraud measures slower to develop than the economy, this creates a gap in the market and an opportunity for FDP players to cater to this emerging and growing demand
Challenges / Headwinds	Limited budget for FDP solutions	<ul style="list-style-type: none"> Vietnam has a low estimated fraud and risk management budget of US\$ 75 M per company On average, the estimated budget for new fraud prevention technology in APAC in 2020-21 is at US\$ 83 M, ~11% more than that of Vietnam
	Lack off real-time data availability	<ul style="list-style-type: none"> More real-time third-party data is needed to help firms better balance speed of approval against customer abandonment before transaction completion

Source(s): GBG and The Asia Banker (Survey of N=324 of financial institutions), Secondary research, Praxis analysis

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

FDP market landscape in Southeast Asia

FDP market landscape in Singapore

FDP market landscape in Indonesia

FDP market landscape in Malaysia

FDP market landscape in Vietnam

FDP market landscape in Thailand

FDP market landscape in Philippines

FDP playbook

Appendix

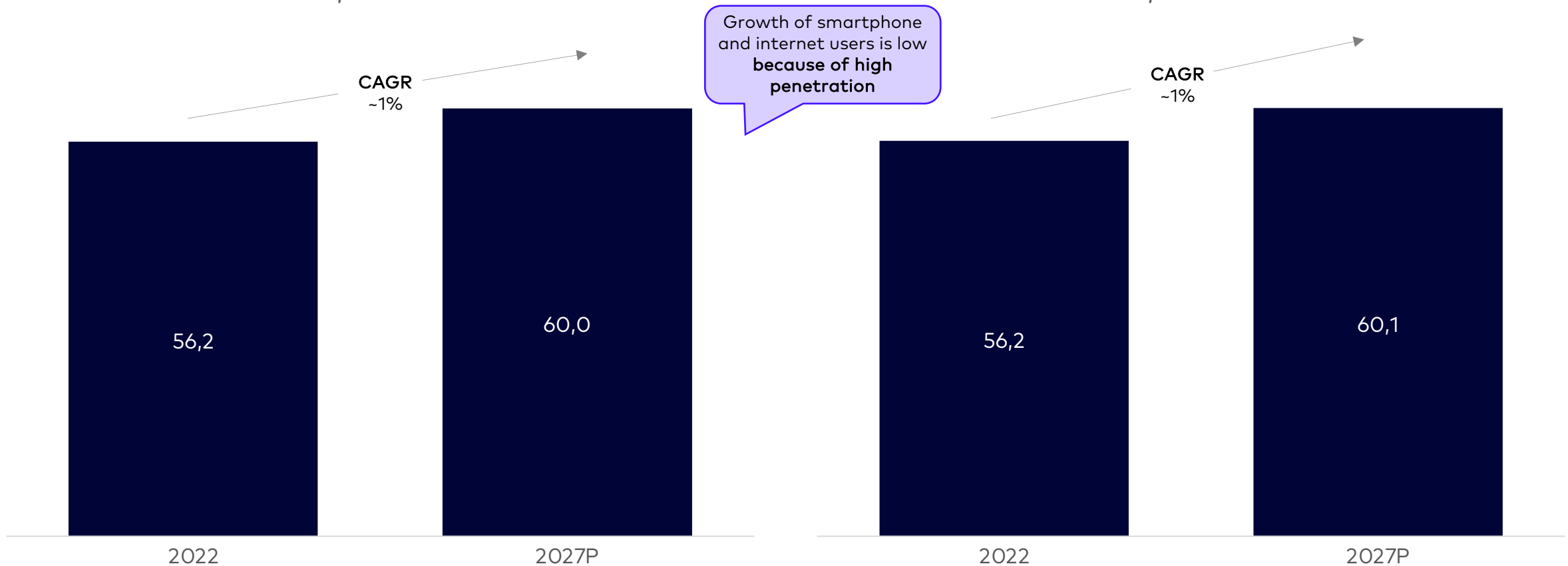
Smartphone users and internet users were both ~56.2M in 2022 and are expected to reach ~60M and ~60.1M respectively by 2027

Smartphone users are expected to reach ~60M by 2027, growing at a CAGR of 1%

Internet users are expected to reach ~60.1M by 2027, growing at a CAGR of 1%

Smartphone users
In M, 2022 - 27P

Internet users
In M, 2022 - 27P



Source(s): Statista, World bank, Secondary research, Praxis analysis

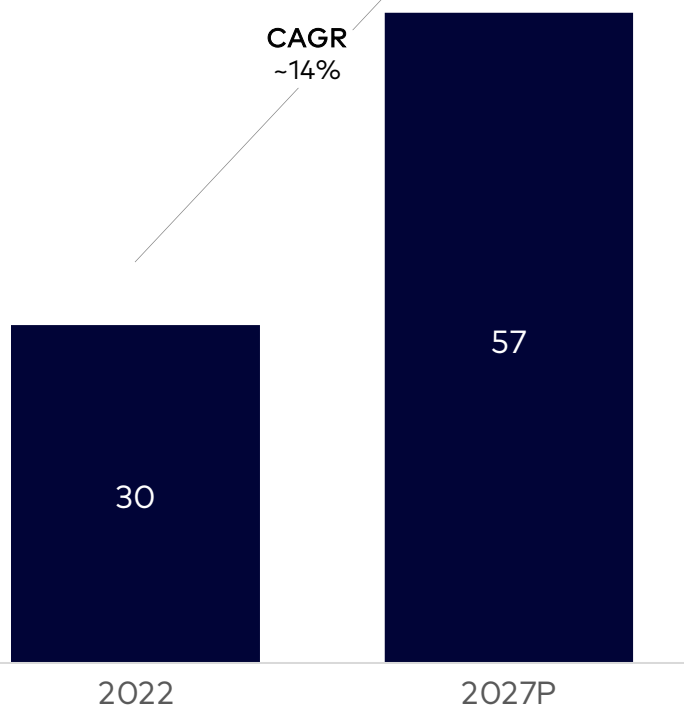
Digital transaction volume to reach ~38B by 2027; credit cards accounted for ~30% of the total digital transactions in 2021

Digital transactions value is expected to increase to ~US\$ 57B by 2027

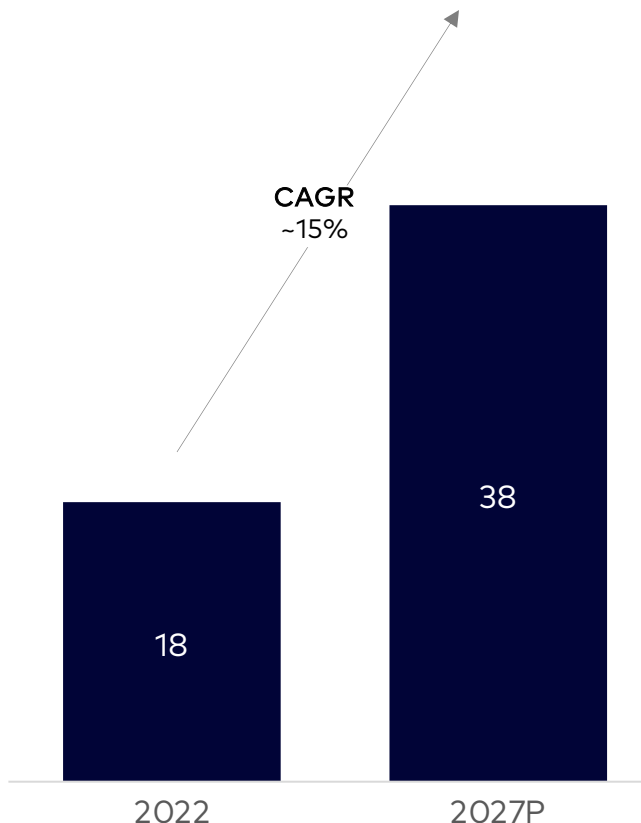
Digital transactions volume is expected to be ~38B in 2027, growing at ~15% CAGR

~ 30% digital transactions happen through credit cards

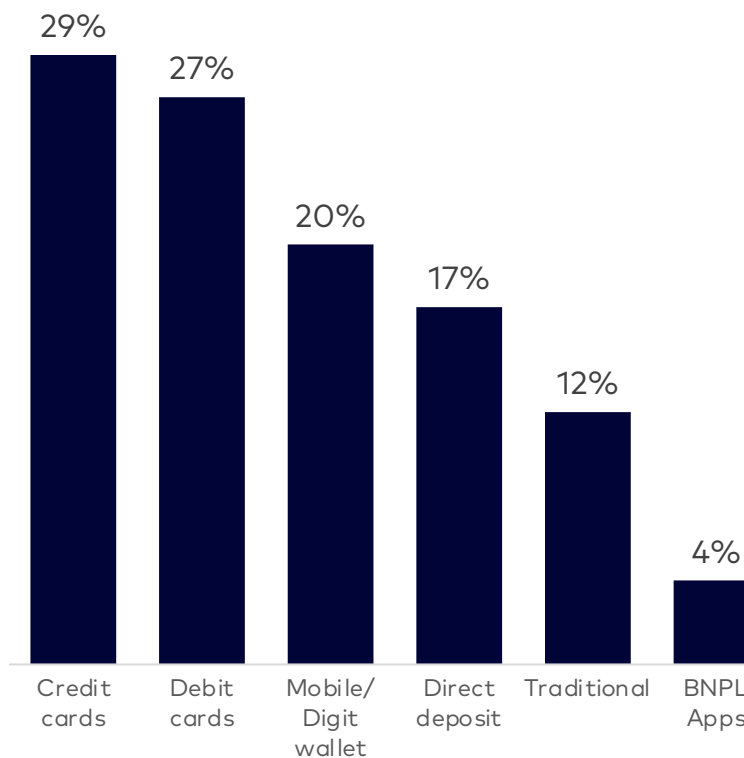
Value of digital transactions in Fintech
In US\$ B, 2022 - 27P



Volume of digital transactions
In B, 2022 - 27P



Transaction volume across payment methods
In %, 2021
N = 120



Source(s): Statista, ACI worldwide, LexisNexis industry report (survey of N = 120 fraud and risk executives across industries), Secondary research, Praxis analysis

Fraud costs banks and financial services 5X the value of fraud which is largely contributed by transactions

Cost of fraud for unit amount lost in transaction is more than US\$ 5 in FS

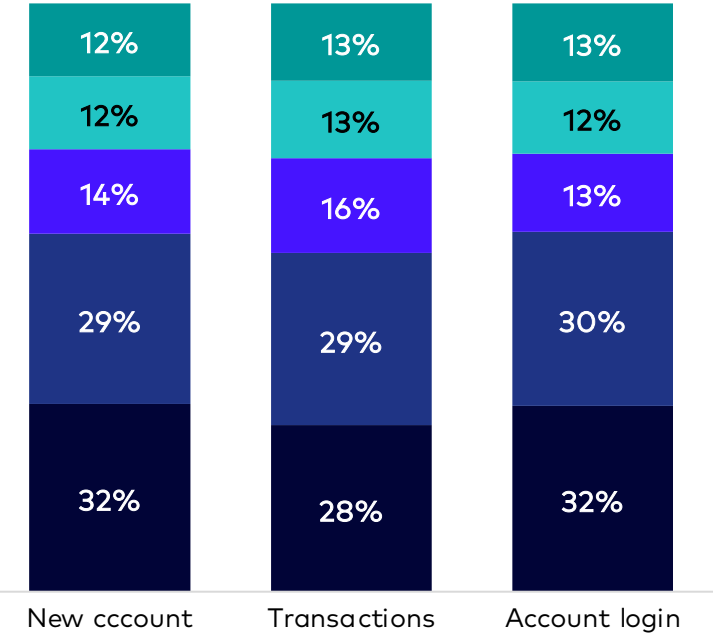
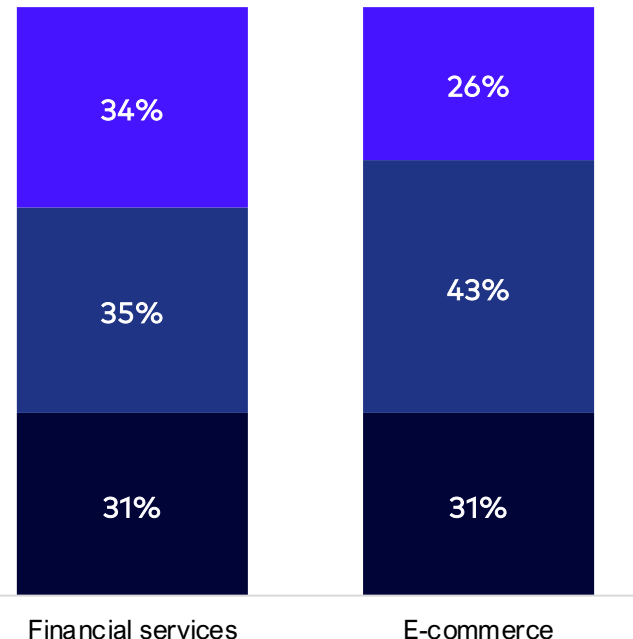
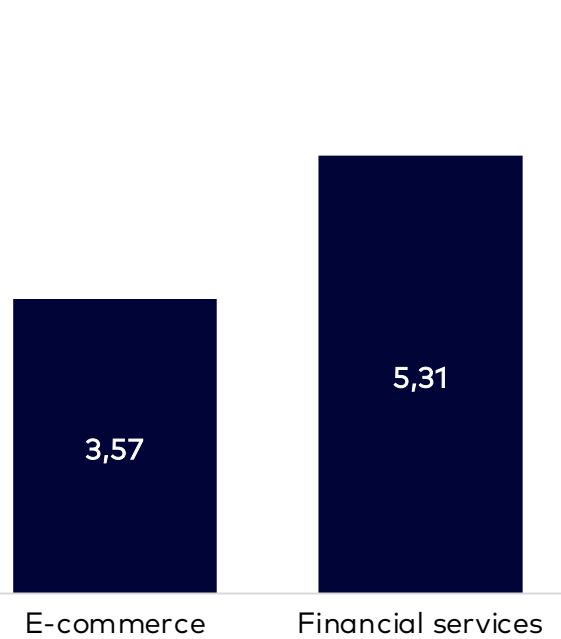
Fraud costs across customer journey is dominated by transactions

Synthetic identity and friendly fraud losses constitute more than 55% of total losses

Cost of fraud for unit amount lost in transaction
In US\$, 2022
N = 120

Fraud costs by customer journey stage
In %, 2022
N = 120

Distribution of losses by fraud type
In %, 2022
N = 120



APAC avg. (US\$)	E-commerce	Financial services
	3.56	5.24

■ New account creation ■ Transactions ■ Account login

■ Lost / stolen merchandise
■ Fraudulent request for return / refund
■ 3rd party account takeover
■ Friendly / 1st party fraud
■ 3rd party / Synthetic identity fraud

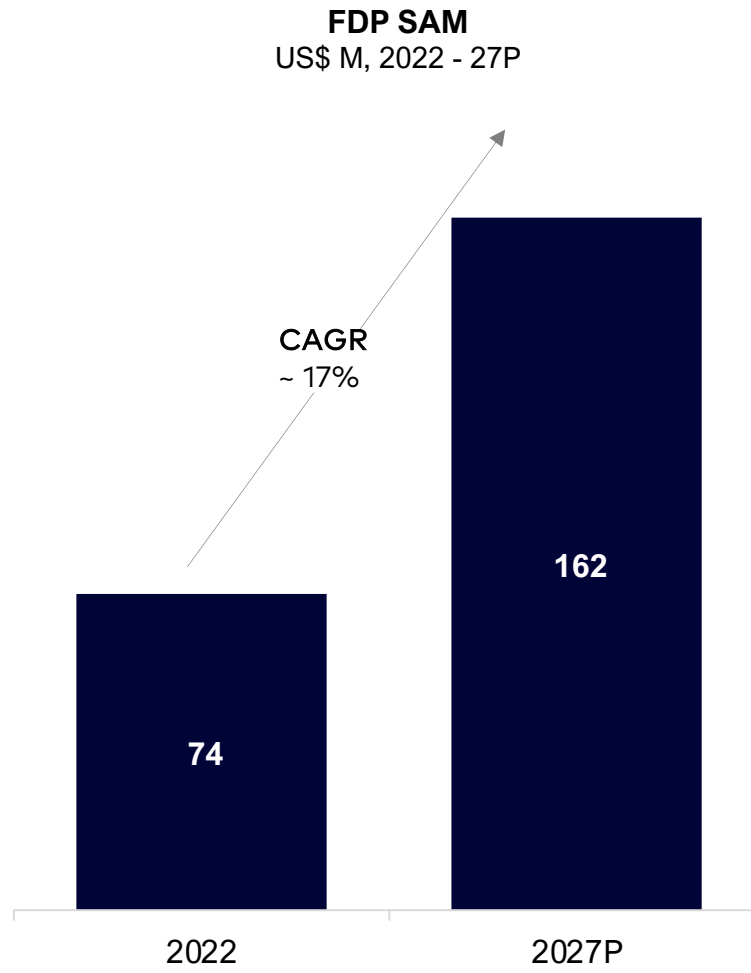
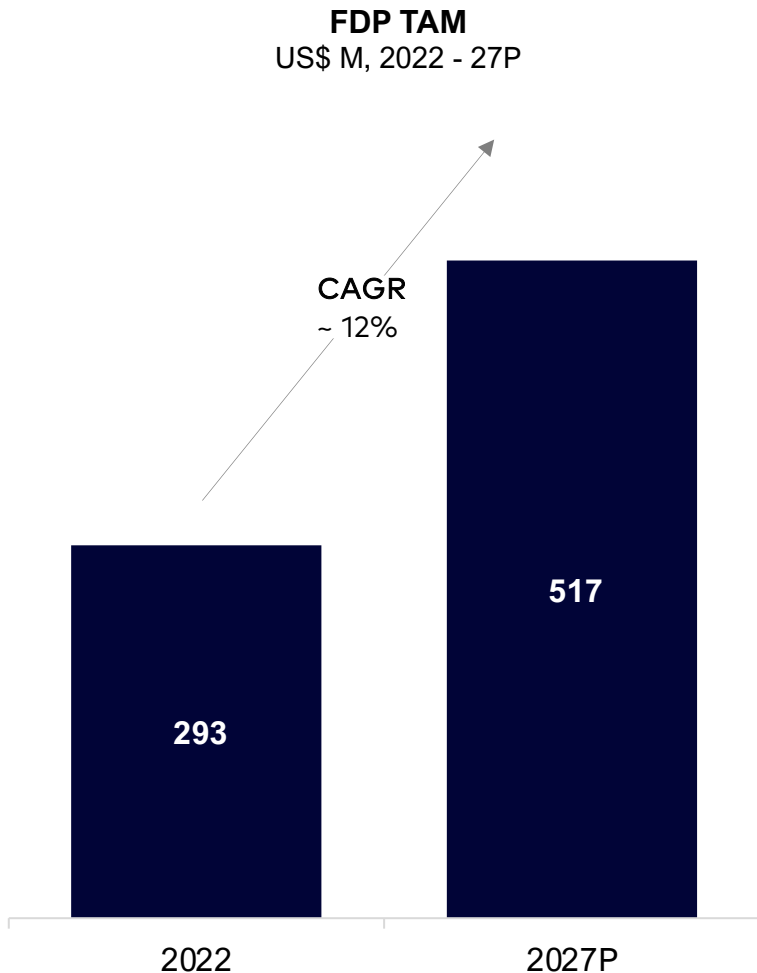
Source(s): LexisNexis industry report (survey of N = 120 fraud and risk executives across industries), Secondary research, Praxis analysis

Of the total US\$ 293M addressable FDP market, ~US\$ 74M was the serviceable addressable FDP market in 2022

FDP TAM was ~US\$ 293M in 2022 and is expected to be ~US\$ 517M in 2027

FDP SAM was ~US\$ 74M in 2022 and is expected to be ~US\$ 162M in 2027

Rise in internet and e-commerce penetration are the top growth drivers



Growth factor	Details
Increasing internet penetration	<ul style="list-style-type: none"> Internet penetration stands at 81% in 2022, which is expected to drive the adoption of internet-related services and eventually FDP solutions
Increasing e-commerce penetration	<ul style="list-style-type: none"> Pandemic pushed customers to purchase online and provided them with the convenience of online platforms Post pandemic customers chose using the online platforms rise to fraud vulnerabilities
Credit card fraud rates	<ul style="list-style-type: none"> Credit card fraud rates are growing at a rate of 20% annually → increase in demand for FDP solutions
Emergence of big data analytics	<ul style="list-style-type: none"> Big data analytics uses advanced analytics techniques like AI and ML, allowing organizations to prevent advanced fraud

Note(s): FDP TAM is the overall FDP market, whereas the FDP SAM includes the total outsourced market
 Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Inadequate data standardization are the main challenges whereas growth in real-time payments and migration to digital solutions are the major opportunities

Opportunities / Tailwinds	Growth in real-time payments	<ul style="list-style-type: none"> Thailand has shown a significant growth in real-time payments; its volume is projected to reach 32B by 2027 from ~11 B in 2022, growing at 23% This is expected to drive demand for real time transaction monitoring FDPs
	Advancement in technology	<ul style="list-style-type: none"> The outbreak of Covid-19 pandemic accelerated the digital transformation process for businesses which create a broad scope for digital fraud In Thailand, government agencies worked with private sector to create unmatched digital infrastructure bringing in abundance of digital data which gets exposed to plethora of fraud vulnerabilities creating a need for advanced FDP solutions
	Migration to digital solutions for onboarding and transaction monitoring	<ul style="list-style-type: none"> The organizations have started onboarding customers digitally and looking to invest in transaction and payments fraud management solutions The volume of digital transactions were ~18B in 2022 and expected to grow at a CAGR of ~15% pushing companies to improve their fraud detection capabilities to prevent probable fraud due to digital transactions
Challenges / Headwinds	Inadequate data standardization	<ul style="list-style-type: none"> The lack of data standardisation and governance is a cause for ineffective fraud risk investigation Deployment of FDP solution becomes difficult because of data standardization issues
	Big data and machine learning are not implemented	<ul style="list-style-type: none"> In majority of the organizations big data and machine learning is not implemented for transaction monitoring FDP players face challenges to deploy an advanced FDP solution in the absence of big data and ML capabilities
	Increasing complexity of fraud attacks	<ul style="list-style-type: none"> Fraudsters are becoming more advanced in finding loopholes in the systems and commit complex fraud creating challenges for FDP players in terms of development or improvisation of existing services they offer
	Data privacy risks	<ul style="list-style-type: none"> Deployment of a FDP solution requires thorough understanding of the client’s system for effective fraud management but due to data privacy concerns clients are apprehensive in disclosing confidential data and hence building trust with clients is becoming challenge for FDP players

Source(s): Secondary research, Praxis analysis

Agenda

Introduction

FDP overview

Global adoption of FDP

India FDP market landscape

FDP market landscape in Southeast Asia

FDP market landscape in Singapore

FDP market landscape in Indonesia

FDP market landscape in Malaysia

FDP market landscape in Vietnam

FDP market landscape in Thailand

FDP market landscape in Philippines

FDP playbook

Appendix

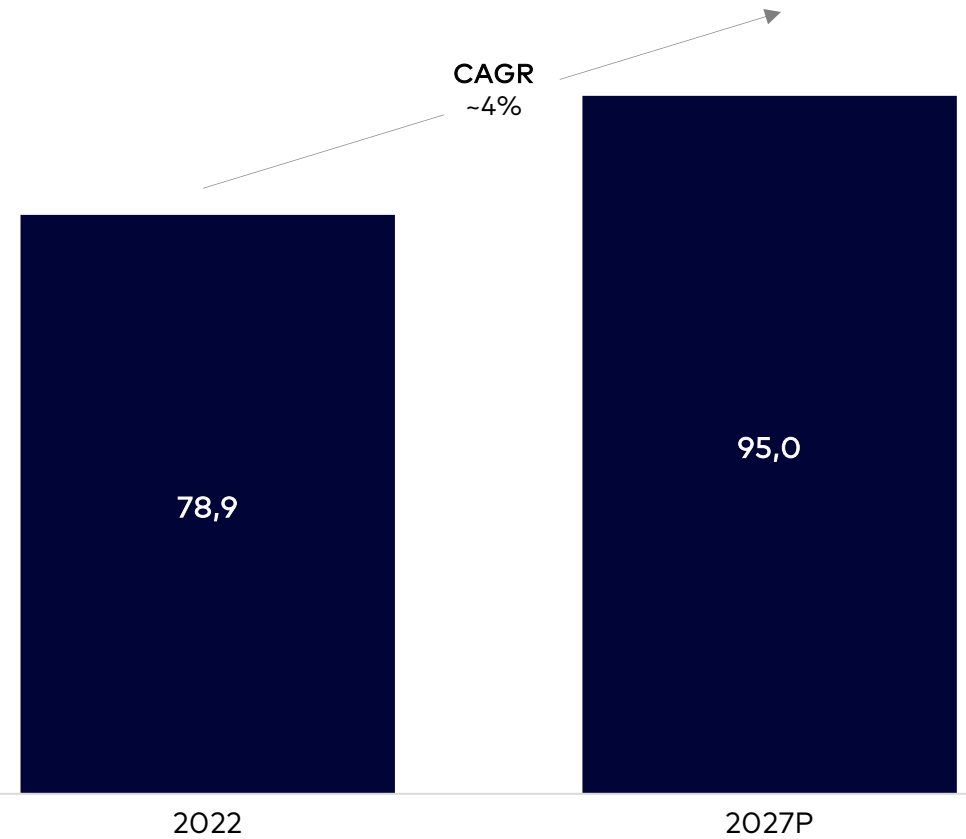
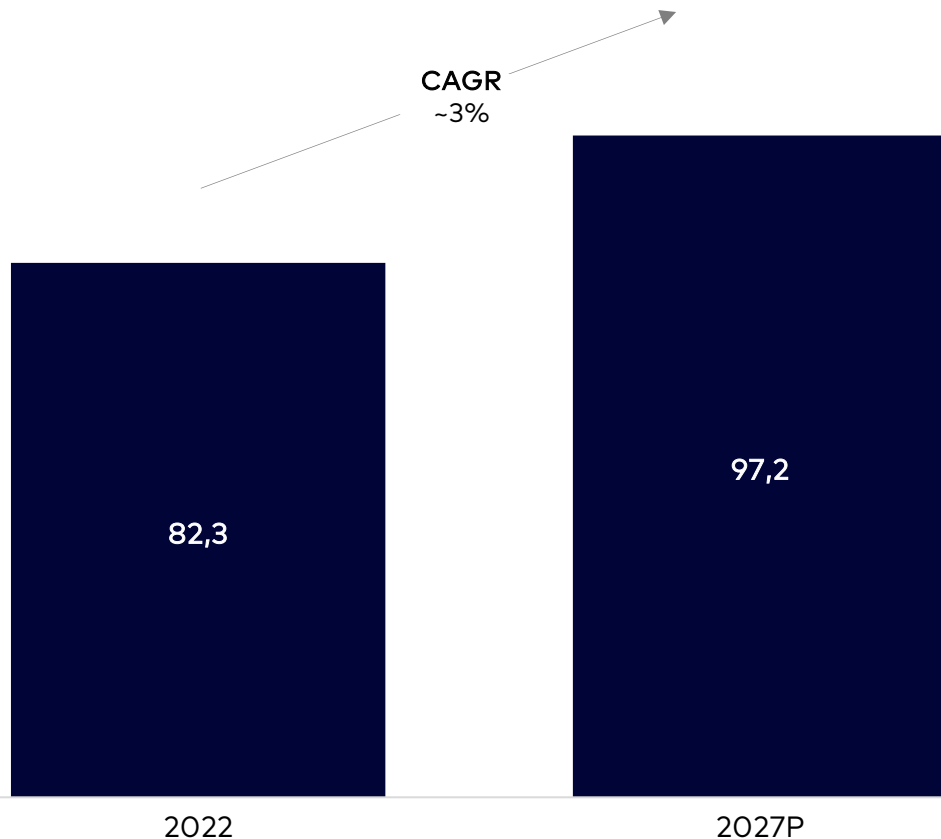
Smartphone users and internet users were ~82.3M and ~78.9M respectively in 2022 and are expected to reach ~97.2M and ~95M respectively by 2027

Smartphone users are expected to reach ~97.2M by 2027, growing at a CAGR of 3%

Internet users are expected to reach ~95M by 2027, growing at a CAGR of 4%

Smartphone users
In M, 2022 - 27P

Internet users
In M, 2022 - 27P



Source(s): Statista, World bank, Secondary research, Praxis analysis

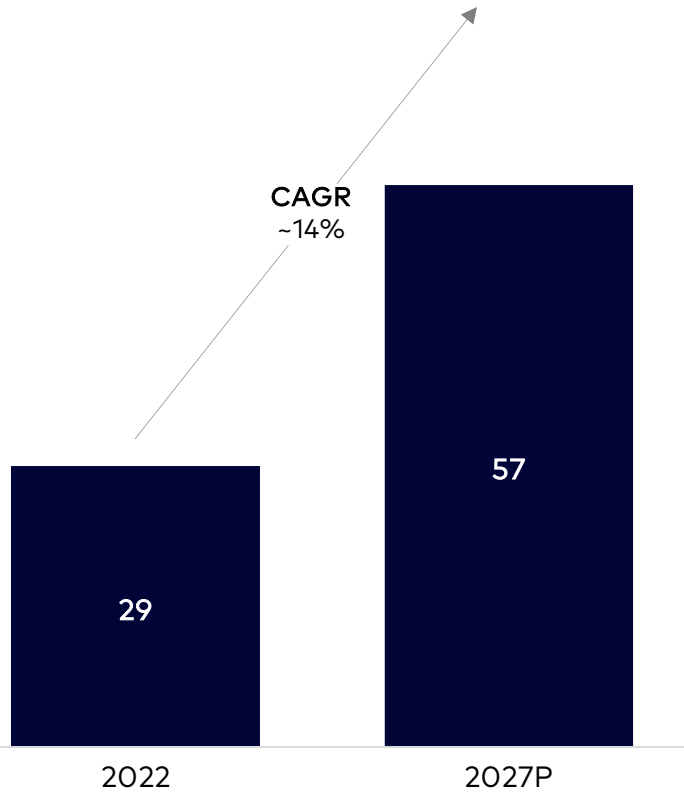
Digital transaction volume to reach ~3.7B by 2027; credit cards accounted for ~30% of the total digital transactions in 2021

Digital transactions value is expected to increase to ~US\$ 57B by 2027

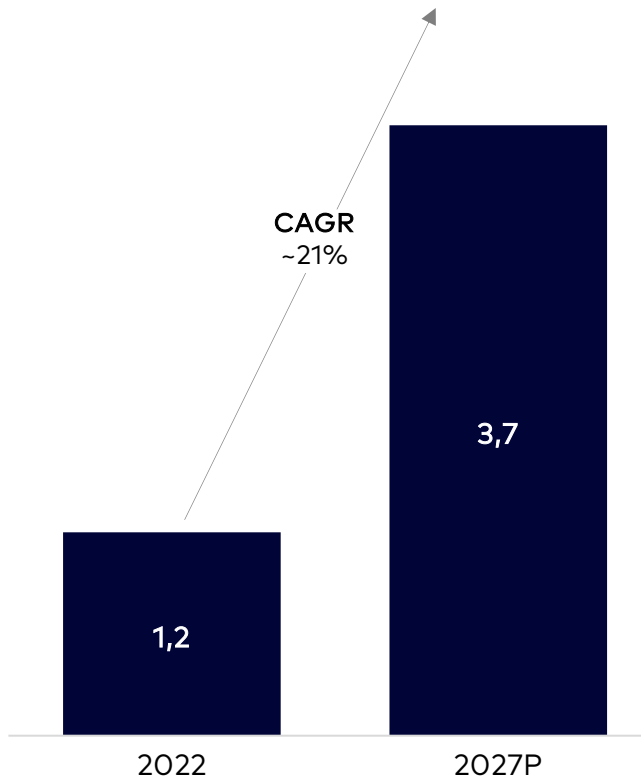
Digital transactions volume is expected to be ~3.7B in 2027, growing at ~21% CAGR

~50% transactions happen through cards whereas ~20% happen through mobile wallet

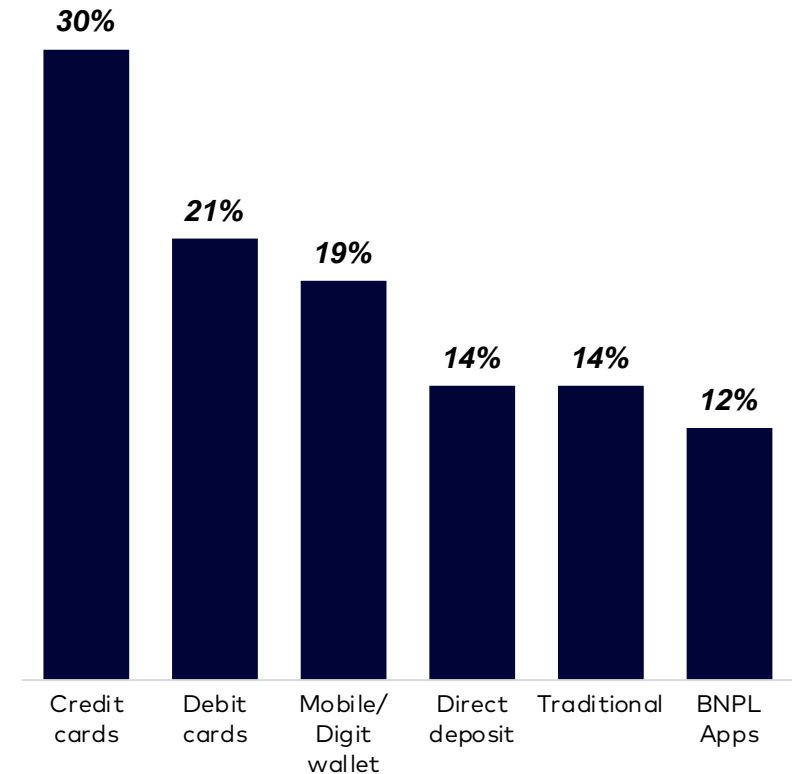
Value of digital transactions in Fintech
In US\$ B, 2022 - 27P



Volume of digital transactions
In B, 2022 - 27P



Transaction volume across payment methods
In %, 2021
N = 120



Source(s): Statista, ACI worldwide, LexisNexis industry report (survey of N = 120 fraud and risk executives across industries), Secondary research, Praxis analysis

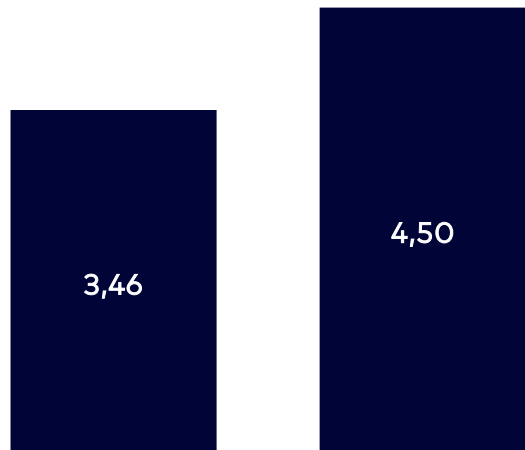
Fraud costs banks and financial services 4.5X the value of fraud which is largely contributed by transactions

Cost of fraud for unit amount lost in transaction is ~US\$ 4.5 in FS

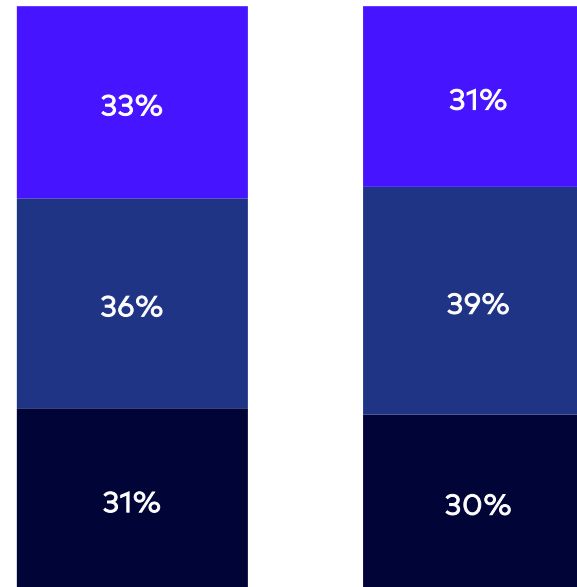
Fraud costs across customer journey is dominated by purchase transactions

Synthetic identity and friendly fraud losses constitute more than 55% of total losses

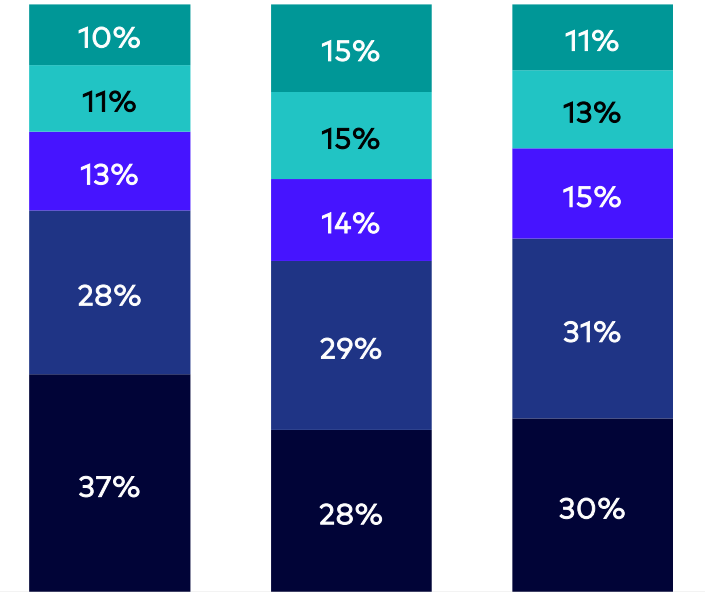
Cost of fraud for unit amount lost in transaction
In US\$, 2022
N = 120



Fraud costs by customer journey stage
In %, 2022
N = 120



Distribution of losses by fraud type
In %, 2022
N = 120



APAC avg. (US\$)

3.56

5.24

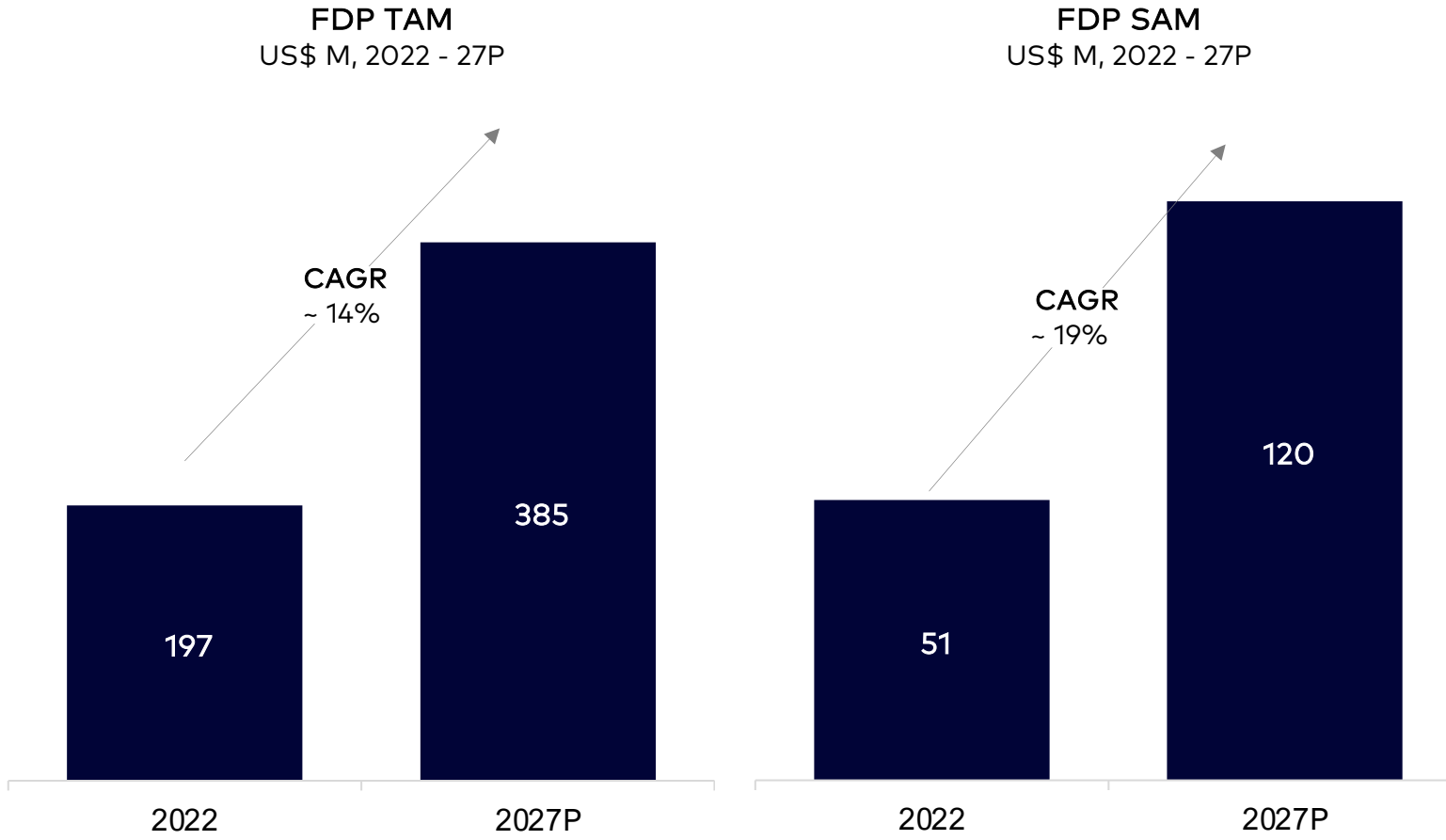
Source(s): LexisNexis industry report (survey of N = 120 fraud and risk executives across industries), Secondary research, Praxis analysis

Of the total US\$ 197M addressable FDP market, ~US\$ 51M was the serviceable addressable FDP market in 2022

FDP TAM was ~US\$ 197M in 2022 and is expected to be ~US\$ 385M in 2027

FDP SAM was ~US\$ 51M in 2022 and is expected to be US\$ 120M+ in 2027

Rising digital payment adoption, shift to digital channels, BSP mandates are the key drivers



Growth factor	Details
Increase in digital payments	<ul style="list-style-type: none"> Digital payments form ~30% of total retail payments in 2021, up from ~20% share in 2020
Shift to digital channels	<ul style="list-style-type: none"> Cybercriminals have taken advantage of more Filipinos shifting to mobile apps Rapid technological advancements in the fields of AI / ML, IoT etc. have also led to growing number of digital apps
BSP* mandate	<ul style="list-style-type: none"> Financial institutions offering electronic payments and financial services must undergo the BSP's approval process Further BSP has been developing a circular requiring the adoption of strong fraud management systems and temporary freezes on funds
Fraud are becoming more sophisticated	<ul style="list-style-type: none"> With fraud becoming more complex, businesses are looking for a robust fraud and security technology platform, offering strong fraud management

Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Growing fintech penetration, government push are the drivers of FDP solutions adoption whereas latency issues, weak digital infrastructure are the main challenges

Opportunities / Tailwinds	Fintech penetration	<ul style="list-style-type: none"> The penetration of Fintech services reached ~49% in 2021, making it almost every second Filipino currently using at least one Fintech service → greater opportunity for FDP players
	Government push	<ul style="list-style-type: none"> BSP* target of achieving 70% account ownership → rapid digital shift and hence, boosting the demand for FDP solutions Financial institutions are now required to have an automated and real-time fraud monitoring and detection system to address the growing incidents of digital fraud
	AI / ML adoption	<ul style="list-style-type: none"> As AI / ML are becoming more common, businesses are looking for a continuous cycle of monitoring, detection, decisions, case management → greater opportunity for FDP players
	Increasing fraudulent activities in banks and financial institutions	<ul style="list-style-type: none"> Fraud management solutions are becoming more crucial in banks and financial institutions owing to the dramatic increase in fraudulent activities Banks are actively looking for fraud management tools; many banks in the Philippines have adopted telco data-based fraud authentication and verification tools to reduce fraudulent credit card and loan applications
Challenges / Headwinds	Latency issues	<ul style="list-style-type: none"> Due to latency issues, complex fraud detection often cannot be completed in real-time
	Weak digital infrastructure	<ul style="list-style-type: none"> Weak digital infrastructure, high internet cost, and uneven quality of the internet are hampering the effective use of digital technologies
	Data constraints	<ul style="list-style-type: none"> Non – exhaustive and poor-quality data makes difficult for FDP players to identify and prevent fraud efficiently

Agenda

Introduction

FDP overview

Global adoption of FDP




India FDP market landscape

FDP market landscape in Southeast Asia

FDP playbook

Appendix

Many FDP players have evolved from different starting points to develop end-to-end capabilities

		Identity protection – API (analytics)	ID and user record database (e.g. bureaus)	Transaction monitoring	Orchestration ¹
Global FDP players		✓	✓	✓	✓
		✓	✓	✓	✓
		✓	✗	✓	✗
		✓	✓	✓	✓
		✓	✓	✓	✓
Indian FDP players		✓	✓	✓	✓
		✓	✗	✓	✓
		✓	✗	✗	✗
		✓	✗	✗	✗

Note(s): 1. A solution that connects tools producing risk and trust signals to underlying analytics tools, and provide step-up authentication in response
 Source(s): Company websites, Industry reports, Secondary research, Praxis analysis

Starting point

Six key areas FDP players should focus on to create an efficient and accurate fraud detection and prevention model

1

Machine learning enabled solutions instead of static rules-based systems

- When fraudsters adopt new tactics or customers change their usage pattern and behaviors, ML models **ingest and analyze these signals and create alerts in real-time**
- Accuracy of ML solutions improves with the increase of usage and data

2

Multi-layered solution approach

- A multi-layered, strong authentication defense approach is needed as single point protection is no longer enough and results in single point of failure
- Includes a **single authentication decision platform** that incorporates **real-time event data, third-party signals, cross-channel intelligence**

3

Right balance

- Striking the balance between **frictionless customer experience and robust security** is the key
- **Frictionless CX** like seamless onboarding, one-click checkout, frictionless authentication **increases customer LTV, improves brand loyalty, reduces drop-offs** from SMS OTP delivery failure

4

Real-time monitoring

- Real-time monitoring and tracking tools help in **proactively monitoring fraud** by analyzing 500+ device metrics, biometrics and user behavior
- RTM also helps in significantly improving **fraud detection accuracy**

5

Focusing on multiple attributes

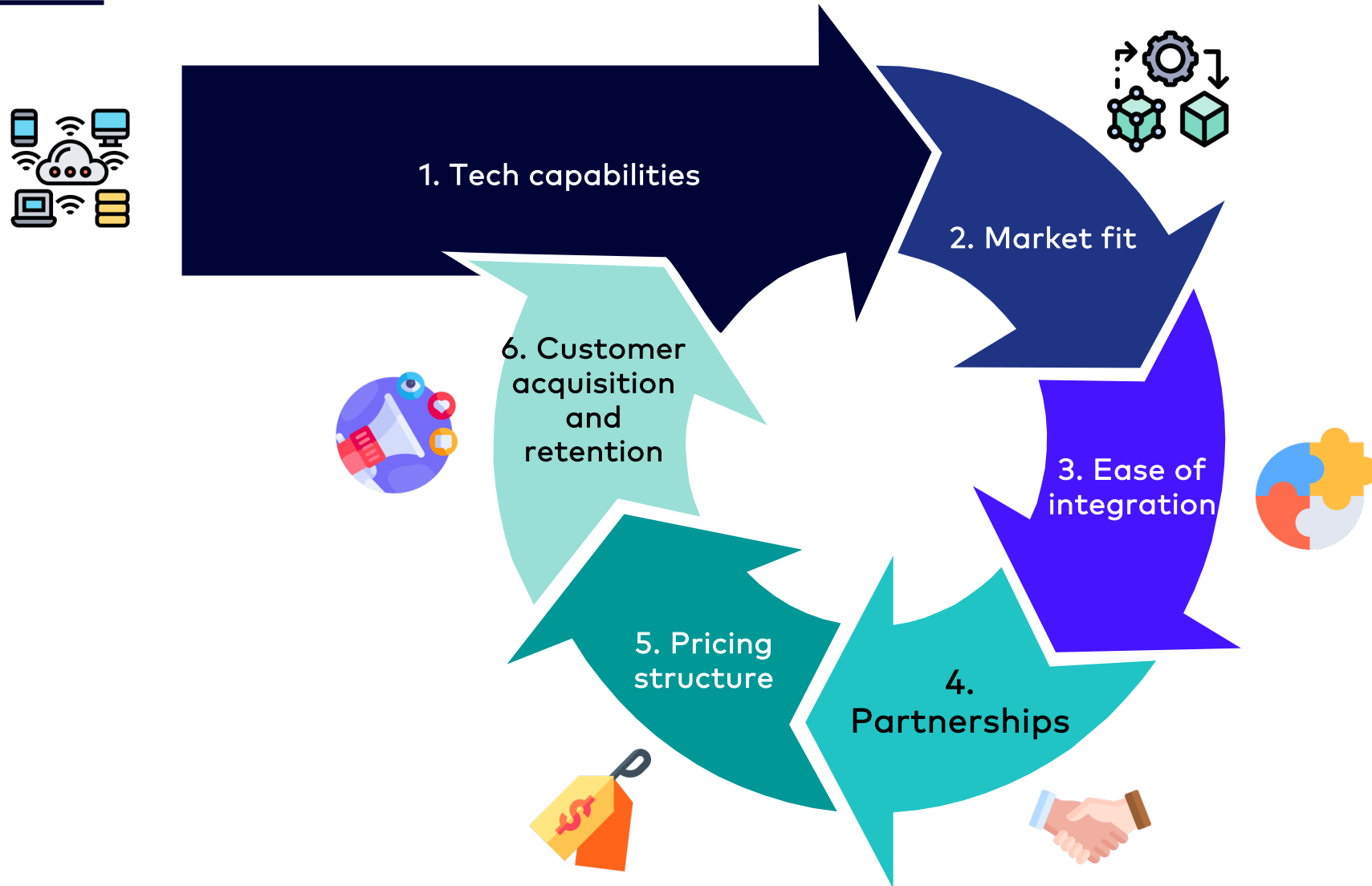
- Assessing various attributes like **physical identity attributes, behavioral attributes, keystroke dynamics, users' login from multiple devices, locations and channels among others** for efficient fraud detection and prevention

6

White box machine learning

- **Sophisticated whitebox algorithms** are considered central to the fight against fraud both in terms of fraud prevention and detection
- Whitebox machine learning algorithms give clearly **readable rules along with the decision and result**
- Ability to **tweak and adapt decision processes**, optimizing and improving the output at will, where needed
- Humans have the final say on the results, so **accuracy is high**

FDP players need to focus on 6 key areas to expand operations, gain product maturity and increase market share



1

Real-time monitoring, behavioral biometrics, predictive analytics, and white-box ML are key techniques used to achieve frictionless experience & robust detection

Technique		Brief description	Impact on fraud detection accuracy	FDP platforms using this technique
Physical biometrics		<ul style="list-style-type: none"> Analyzes parameters such as - fingerprint, facial parameters or voice 		
Behavioral biometrics		<ul style="list-style-type: none"> Behavioral biometric authentication includes keystroke dynamics, gait analysis, cognitive biometrics, and signature analysis 		
Advanced AI / ML	Blackbox ML	<ul style="list-style-type: none"> Designed to work in a 'set and forget' mode, where the decisions are opaque and automated Great for small businesses 		
	Whitebox ML	<ul style="list-style-type: none"> Gives you clear explanations as to why a risk rule was suggested Makes it easier to understand where the risk is and gives fraud managers more flexibility to improve their fraud prevention strategy 		
Rules-based system		<ul style="list-style-type: none"> Requires manual tuning to adapt to new data Risky users can fail to trigger rules based on known patterns, resulting in high false positive and false negative rate 		
Real-time monitoring		<ul style="list-style-type: none"> Real-time risk scores to identify fraud quickly 		
Blockchain / distributed ledger technology		<ul style="list-style-type: none"> With blockchain, one can share the recorded data in real-time and update it with the approval of all parties who have access to the data 		
Predictive analytics		<ul style="list-style-type: none"> Analyzing past data, trends, and variables, to build accurate fraud score algorithms and model 		

Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

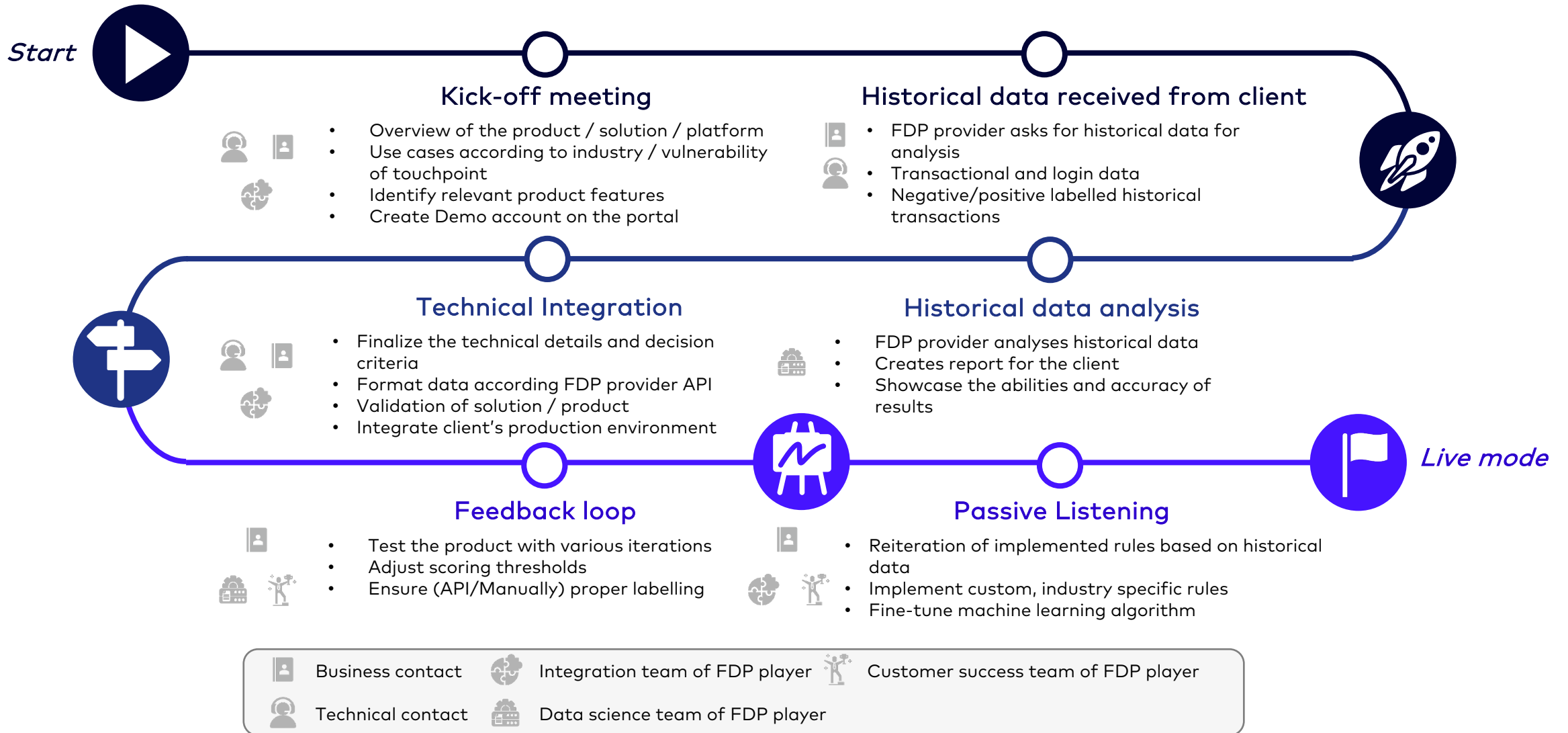


FDP players help enterprises in addressing several gaps in their current fraud detection and prevention capability

	Most common deployment model	White space	How can FDP players help in filling white spaces
Banking	<ul style="list-style-type: none"> • Inhouse for legacy players 	<ul style="list-style-type: none"> • Limited data access • Static approaches (depends only on historic data) • Disparate teams for fraud detection and prevention → latency 	<ul style="list-style-type: none"> • Strong API for sourcing large databases from multiple channels (like bureaus, aggregators, telcos) • Real-time login and transaction monitoring • Orchestration capability
Financial services	<ul style="list-style-type: none"> • Outsourcing for new-age digital fintech companies and neobanks 	<ul style="list-style-type: none"> • Limited data access • Weak identity verification process • Lack of end-to-end solutions for monitoring fraud across the digital customer journey 	<ul style="list-style-type: none"> • Strong API for sourcing large databases from multiple channels (like bureaus, aggregators, telcos) • Real-time login and transaction monitoring • Behavioral and physical biometrics • Robust keystroke dynamics system • Orchestration capability • AI / ML expertise to detect and prevent fraud across customer journey
Insurance	<ul style="list-style-type: none"> • Inhouse largely for legacy players • Outsourcing for new-age digital players 	<ul style="list-style-type: none"> • Inability to efficiently detect and prevent claim related fraud 	<ul style="list-style-type: none"> • Device fingerprinting • Behavioral biometrics
E-commerce	<ul style="list-style-type: none"> • Outsourcing for internet first brands • Inhouse for large e-commerce platforms 	<ul style="list-style-type: none"> • Weak transaction monitoring system • Difficulty in tracking RTO and chargeback fraud • High false positive rate 	<ul style="list-style-type: none"> • Behavioral biometrics • Guarantee model • Ensures low false positive rate
Real money gaming	<ul style="list-style-type: none"> • Inhouse 	<ul style="list-style-type: none"> • Post-facto monitoring 	<ul style="list-style-type: none"> • Real-time monitoring capability

3

Integration of FDP solution predominantly consists of 6 stages, post which the solution goes live



Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

Integration with current fraud detection and prevention systems and intuitive UI/UX are some of the main features that FDP players should be focus on

Features	Details	Current maturity of FDP players	
UI / UX	<ul style="list-style-type: none"> • Availability of features like search function, logging function, workflow creation, reporting, custom rules engine etc. • Dashboard should be clean , intuitive and noise-free, will help in more efficient and quicker decision making 		<p><i>"Backward integration is one the most important criteria we look at while analyzing an FDP solution. We don't want to hamper our internal processes much and the solution should easily be able to blend into the existing system"</i></p> <p><i>-Risk and fraud Head, Leading bank</i></p>
Ease of deployment	<ul style="list-style-type: none"> • Installing and configuring software on numerous on-premise systems can take weeks to complete, leading to prolonged implementation time and complex implementation • 3rd party FDP solutions have much quicker, simpler and speedy deployment 		
Integration with current operations	<ul style="list-style-type: none"> • Fraud detection and prevention methods should blend seamlessly with the existing operational workflows • Enterprises should have easy access to data - shouldn't need months of intensive services support to integrate output with operational workflow • Companies may not want to rebuild everything from the ground up, or they are legally required to keep some data to themselves 		<p><i>"The uptime of the application should be extremely high. We don't want bugs and other problems coming up regularly because that would be a major concern for us"</i></p> <p><i>- Product manager, E-commerce platform</i></p>
Training & support	<ul style="list-style-type: none"> • Integration should be bundled with support and training • Allocation of proper deployment teams and support teams for resolution of queries and training support to the enterprises is optimal 		<p><i>"The product features and capabilities should be intuitive to the team. This way we can ensure less time is spent on understanding the solution and implementation is smooth and frictionless"</i></p> <p><i>- Risk dept head, Insurtech startup</i></p>
Ease of maintenance	<ul style="list-style-type: none"> • Updates, extra features and bug fixes – taken care of by the provider • Roll-out for new features tends to be much faster than with built-in solutions 		

Low High

Source(s): Primary conversations, Industry reports, Secondary research, Praxis analysis

FDP players partner with bureaus, aggregators, telcos for improving their productivity and efficiency

Benefits of maintaining an extensive partner network for FDP players



Easy access to bulk data

- Data is the most important requirement for any FDP player
- Partnering with bureaus give them **access to superior quality bulk data** which helps them improve their services



Standardized processes

- Partnership with **bureaus / aggregators** make services and solutions provided by **FDP players standardized**
- This helps FDP players to make **modifications in their processes** in line with their competitors



Ease of market entry

- Partnership with **legacy systems** gives new FDP players **easier accessibility** to the market as their **visibility gets improved**
- The **client's trust in FDP player** is enhanced when it partners with global bureaus and telcos to strengthen their data availability



Improved tech capabilities

- Partnering with aggregators make FDP players **improve their tech capabilities**
- FDP players must comply with the tech requirements of aggregators which creates a need of having **advanced tech deployment**






5

Majority of FDP players follow an 'API call' based pricing; other pricing structures like guarantee premium are also being increasingly adopted by some FDP players

Pricing model	Description	Adoption
Per API call	<ul style="list-style-type: none"> Used for specific use cases within the customer life journey e.g. KYC, credit check, PAN card verification etc. Largely used during the account creation and login phases of the customer journey Pricing can vary depending on the number of checks required Is both flexible and adaptable and provides transparency on spend 	
Per transaction	<ul style="list-style-type: none"> Fixed price per transaction Unit price reduces as the volume of transactions increase 	
Per user	<ul style="list-style-type: none"> Fixed price per user based on pre-defined type and number of checks and decisioning required Unit price reduces as the volume of transactions increase 	
% of value of transaction	<ul style="list-style-type: none"> Fixed percentage of the transactions monitored Typically, applicable for low-ticket and permissible daily transactions for individuals Has a higher price per unit when compared with others 	
Fixed thresholds	<ul style="list-style-type: none"> Fixed cost for an initial volume of users or transactions, then charged per unit Typically, applicable for small to mid business or for situations where the volume of transactions is uncertain 	
Guarantee premium	<ul style="list-style-type: none"> Premium price assigned for chargeback guarantees in "Return to Origin" use cases Can lead to increased false positives due to stricter rules of fraud detection In case the FDP solution is unable to detect the fraud, it bears the cost of logistics for the transaction 	

Low High

FDP SaaS players need to follow a structured sales process to acquire and retain customers

	1  Lead generation	2  Conversion	3  Nurturing	4  Up-sell / cross sell	5  Contract renewal
Description	<ul style="list-style-type: none"> Reaching out to potential customers through marketing campaigns, channel partners, etc. Inbound leads 	<ul style="list-style-type: none"> Reaching out to interested leads through sales team and on-boarding them as customers 	<ul style="list-style-type: none"> Customer engagement with the platform 	<ul style="list-style-type: none"> Selling higher value products Special bundle deals to facilitate cross-selling products and solutions 	<ul style="list-style-type: none"> Renewal of contract for long term engagement
Output metrics	<ul style="list-style-type: none"> Lead gen channel mix Channel throughput: # of leads generated p.m. Qualification approach Cost Per Lead (CPL) Lead Velocity Rate 	<ul style="list-style-type: none"> Conversion funnel (Qual to demo to trial to purchase) Lead conversion ratio CAC Hunter productivity (new logo ARR / hunter) 	<ul style="list-style-type: none"> Accuracy of fraud detection False positive rate Customer M12, M24, M36 retention rates ARR M12, M24, M36 retention 	<ul style="list-style-type: none"> Quality of accounts acquired (underlying spend growth) Expansion MRR Services attach rate Growth rate of users / account 	<ul style="list-style-type: none"> Proportion of contracts nearing expire renewed on Q-o-Q basis Cohort-wise churn NPS / CSAT
[Sample] Overall assessment	<ul style="list-style-type: none"> Reach-outs through multiple channels Scope for synergies through hunting teams 	<ul style="list-style-type: none"> Demo to sales conversion ratio in line with peers 	<ul style="list-style-type: none"> Retention improvement across industries / geographies 	<ul style="list-style-type: none"> Gradual increase in MRR of accounts with time 	<ul style="list-style-type: none"> CSAT score consistently >90% Retention of key accounts

Source(s): Primary conversations, Praxis analysis

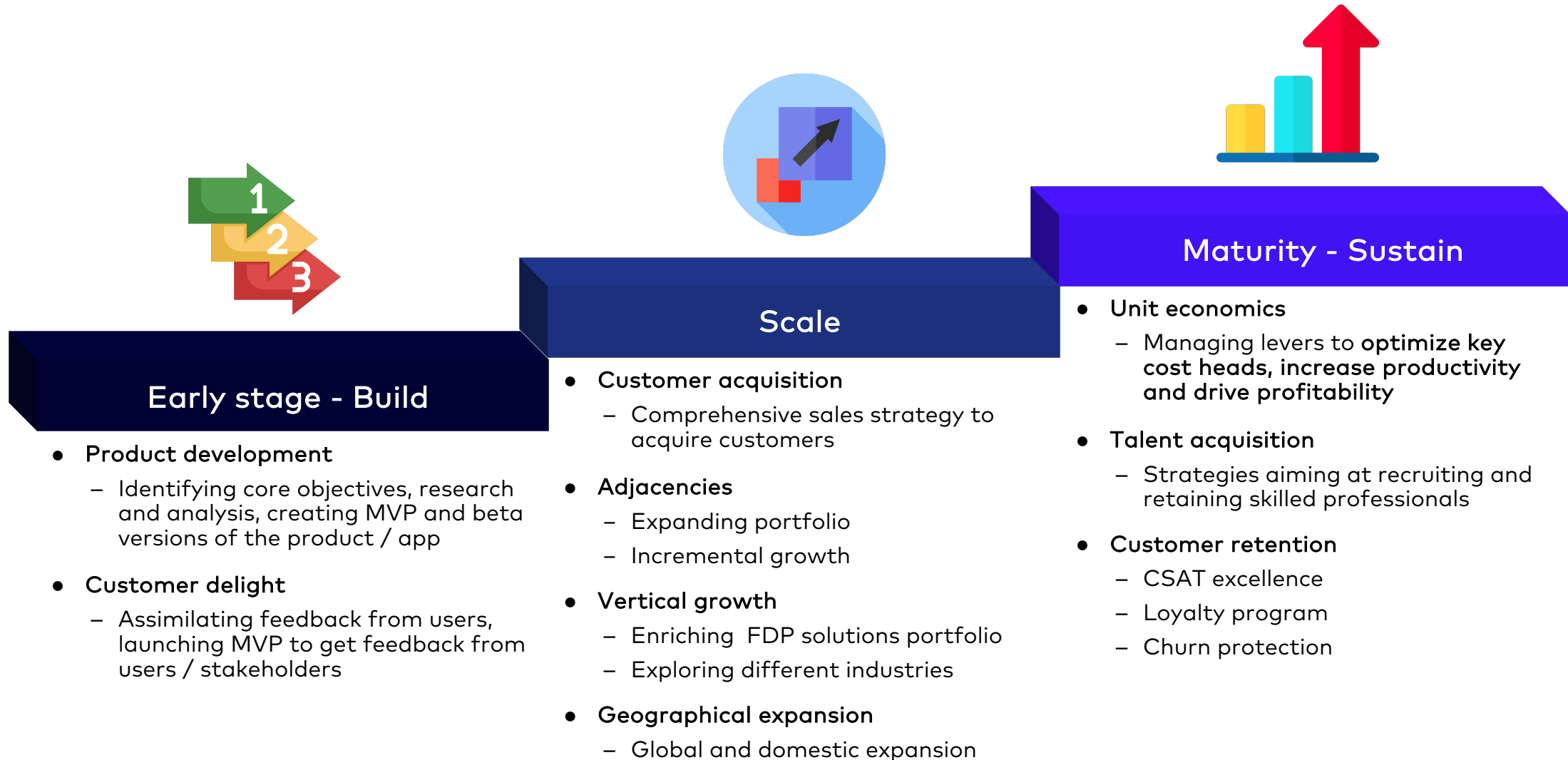
Hunting

Farming

Low  High

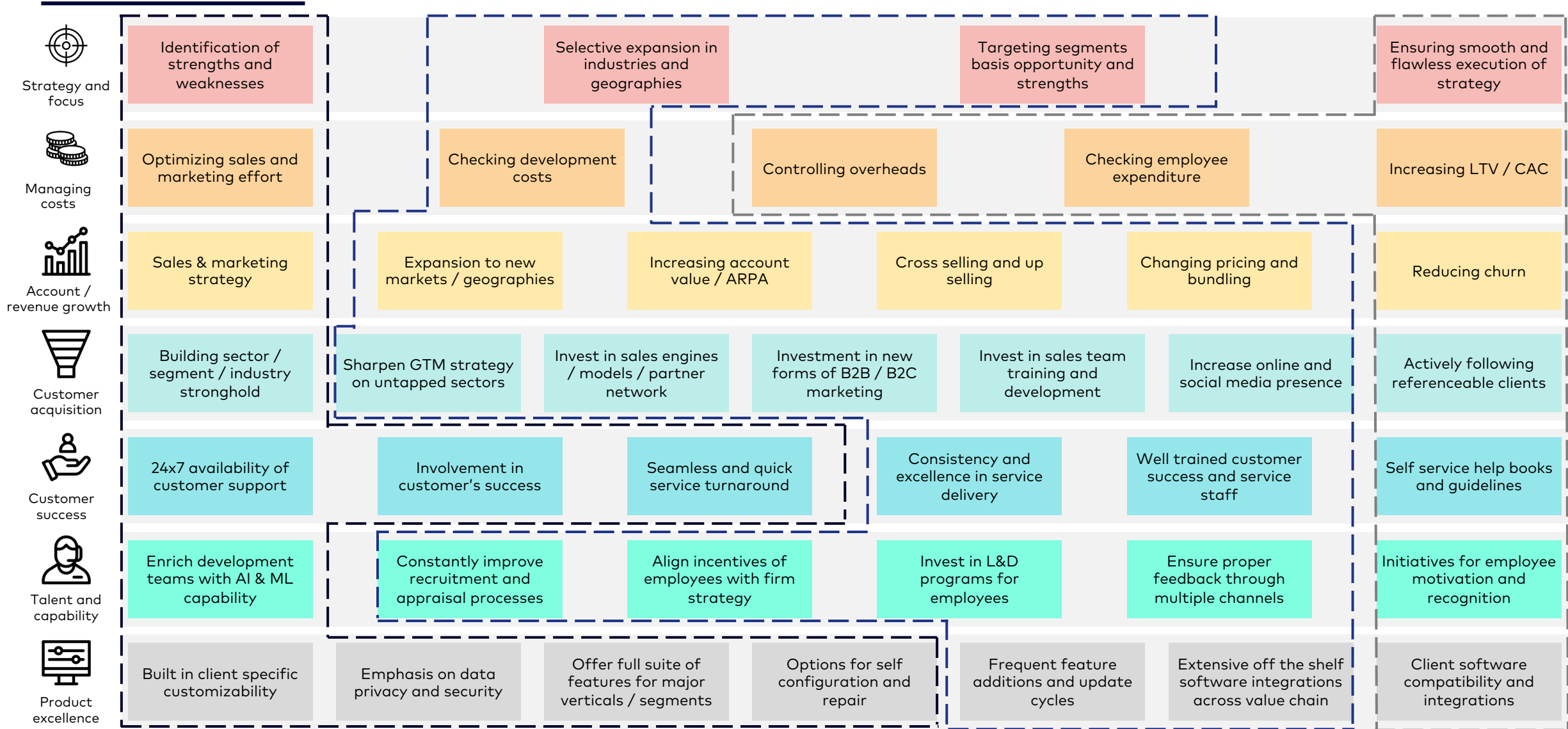
Performance of platform on criteria

Strategic prioritization during different phases in the FDP business life cycle



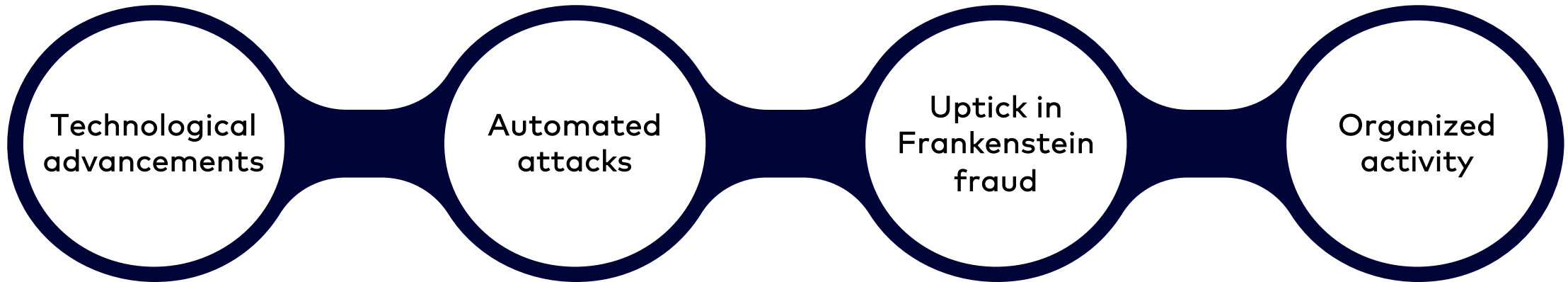
Source(s): Primary conversations, Praxis analysis

What makes a FDP SaaS business successful: Value needs to be created at every step in the business to make it excel globally



Source(s): Praxis analysis

Fraud will become more sophisticated and complex in the future



- Advancements in technology have resulted in fraud attacks occurring with **greater frequency, speed, and effectiveness**
- Rise of **e-commerce, mobile payments, and computing power** is further increasing the risk of fraud
- Fraudsters will increasingly adopt automated methods to make **cyberattacks and account takeovers easier and more scalable** than ever before
- For instance:
 - **Script creation** (using fraudulent information to automate account creation)
 - **Credential stuffing** (using stolen data from a breach to take over a user's other accounts)
- Refers to **synthetic identity fraud**
- Increasing due to multiple factors - **data breaches, dark web data access** and the **competitive lending landscape**
- Fraudsters use **AI** to combine facial characteristics from different people to form a new identity, creating a challenge for businesses relying on facial recognition technology
- Techniques like creating verified accounts with fake documents and then using them in subsequent attacks, point to a more organized attempt
- Subtler signs like – **incorrect fonts, wrong photo printing technique, or imitated security features** can only be identified by **advanced document analysis**

Source(s): Primary conversations, Industry reports, Praxis analysis

FDP players are continuously focusing on enhancing their tech capabilities to provide robust security against new-age evolving fraud



FDP players are striving to strengthen their AI/ML models to predict and detect fraud which are **explainable to the clients as well** – this gives more **reliability to the companies to label the detected fraud**



New-age FDP players are looking to move towards becoming **end-to-end solution providers**, providing a suite of tech capabilities covering **use cases across the customer journey**



Shifting focus to delve into **emerging sectors** such as cryptocurrency, real money gaming and gig economy – **increasing fraud cases and need for accurate FDP solutions** increasing in these industries



FDP players are focusing their investments in establishing technology capabilities **that improve customer experience without compromising security robustness**



FDP platforms are aiming to create an **exhaustive database** of transactions and other customer data fields that provides an **accurate and comprehensive picture of each user** – to make fraud detection strikingly more accurate and efficient

Source(s): Industry reports, Praxis analysis

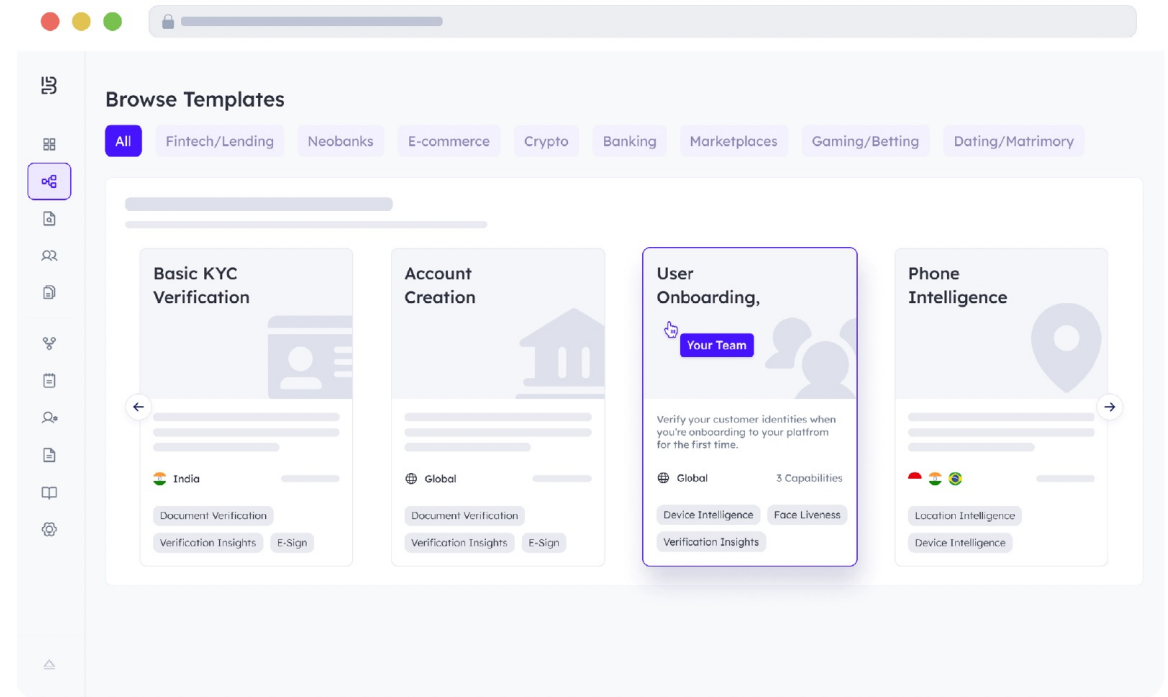
About Bureau

Bureau is a modern no-code decisioning platform. It delivers absolute conclusions about digital identity trustworthiness to prevent fraud, ease compliance, and make it easy for consumers to transact online.

The single AI-architected platform provides banks, fintech, gaming, gig economy and e-commerce companies with a complete range of risk, compliance, fraud prevention and detection, and onboarding solutions.

Its Identity Bureau network supplies customers with insights derived from an identity graph and feedback loop about digital identities based on contextualized linkages. Backed by tier-one investors Okta, Commerce Ventures, Quona, Blume, and Village Global, Bureau is headquartered in San Francisco, CA, with offices in Bangalore, India and Singapore.

Visit www.bureau.id and follow Bureau on [LinkedIn](#).



About Praxis Global Alliance

Praxis Global Alliance is the next-gen management consulting firm revolutionizing how consulting projects are delivered. It delivers practical solutions to the toughest business problems by uniquely combining domain practitioner expertise, AI-led research approaches, and digital technologies. The company operates three business units, including Praxis Global Alliance Financial Investor Group (FIG), offering pre-deal support, commercial due diligence, post-acquisition value creation, Praxis Global Alliance Business Enablement and Transformation (BET) for practitioner-led business advisory and consulting, and PraxDigital™ delivering data engineering and analytics, AI, OpenData and visualization solutions to clients across verticals.

Present in 4 locations in India, Praxis Global Alliance has successfully served 40+ countries with a team of over 200+ consultants and data scientists. Team Praxis works with C-suite to the front-line executives across business streams, helping them with end-to-end business enablement, organizational transformation, and revenue maximization support in an agile environment.

For more details, please visit: <https://www.praxisga.com/>



THANK YOU



Bureau
Complete Trust™