Instant Payments with Google Cloud

Alfredo Dos Santos Head of Partner Engineering ISV EMEA



Keep Instant Payments Up, Keep Fraud Down



An EMEA-wide transition to instant payment services is underway

- Customers want instant gratification
- €200 bn. that could support economic growth is locked in transit in the financial system on any given day*
- EU regulations disrupting the industry in the eurozone
 - Must RECEIVE by Jan 2025 and SEND by Oct 2025
- Challenges for providers
 - Legacy infrastructure / fraud risks
- Opportunities for providers
 - modernisation for competitive advantage





The transition to Instant Payments will impact all aspects of the payments business process

Collect and Process	Store and Analyse	Insights and AI Activation	Threat Detection Hackers Fraudsters
			Scammers
From Batch to Continuous Operations	Ad hoc queries during 24/7/365 services	Incident Management	
Orchestration and Automation	Variable cost database infrastructure	Explanations for Paused Payments	



Increased Processing Risks of Fraud



Regulated Processing Speeds and Emerging Fraud Risks

Require banks and payment services providers to rethink tech strategy





Time-bound end-to-end legal requirement for data intensive processing

3,650 legal entities in scope ⁽¹⁾

Instant payments fraud rates (by value) are about 10 times higher on average than conventional credit transfers

Research by FSI Regulators⁽²⁾

Sources:

(1) European Payments Council <u>Register of SEPA Credit Transfer Scheme Participants</u> 13 May 2024
 (2) European Banking Authority "<u>Opinion on new types of payment fraud and possible mitigants</u>" 29 April 2024



Where to start? A long term strategy on fraud prevention is needed now Help stop the fraud it before it occurs

Short Term Tactics:

Manage the Damage

- Evidence Handling
- Liability Framework Management
- Fraudulent Claim Detection
- Arbitration Processes
- Reimbursement Management
- Account Closures
- Cross-Industry Information Sharing

Long Term Strategy: Stop the Fraud

- Combine **data on customer behaviour** and markers of fraudulent activity to mitigate fraud in real time
- Use Explainable AI to contextualise decision making on paused instant payments
- Optimise systems based on recent data, developing a continuously learning detection and feedback loop



Instant Payments volumes will grow with multiple Use Cases each Use Case is a target for Scams and Frauds





First stage of capability development

Stage One

- A unified Al-ready analytics platform
 - Al-enabled analysis of historical,
 legitimate transactions creates a
 baseline of legitimate customer behaviour
 - Historical behavioural data is a vital step towards real-time fraud detection models

Emerging Instant Payments Use Cases





Second stage - Automation to identify potential frauds in real time when Instant Payments become the "new normal"

Stage Two

The payment services provider can use explainable AI within a real time services architecture to pause potentially fraudulent instant payments that do not follow the historical pattern of legitimate customer behaviour



McKinsey Global Payments Report September 2023



Why Partner with Google & Red Hat



Google Cloud: Your Strategic Partner for Instant Payments Success

Al-enabled analysis of historical, legitimate transactions

Creates a baseline of legitimate customer behaviour

Instant Payments become the "new normal"

Potentially fraudulent instant payments can be paused in real-time, using explainable AI



Instant Payments volumes will grow with multiple Use Cases each Use Case is a target for Scams and Frauds

Person to Person (P2P)

Government to Consumer (G2C)

Instant Payment to Friends and Family

Tax Refunds and Rebates. Government Salaries, Pensions, Social Benefits, Subsidies, Grants, Loans

Consumer to Government (C2G)

Tax Payments, Registration Fees, Loan Repayments

Business to Consumer (B2C)

Rebates, Refunds, Employee Salaries, Employee Expenses, Vouchers, Request for Bill Payment, Insurance Claim Disbursements

Consumer to Business (C2B)

Business to Business (B2B)

Business to Government (B2G)

Government to Business (G2B)

Rebates, Contract Payments



Point of Sale. Remote Location. **Bill Payments, Insurance** Premiums

Supplier Payments, Refunds

Taxes. Fees

Openshift Platform Plus on Google Cloud

Red Hat Red Hat Advanced Cluster Security **Advanced Cluster Management** for Kubernetes for Kubernetes Vulnerability analysis **Application Lifecycle Management** integrates with CI/CD manages Apps pipelines to enable supply deployment and Apps chain security. lifecycle of apps App config analysis **Application deployment** Automate security policies Fleet observability & alerts Vulnerability & Risk profiling Fleet lifecycle management defines, informs and defines, informs enforce security and and enforces Cluster to cluster networking Auto-suggest network policies compliance policies for Apps configuration and applications and Cluster and compliance policies clusters at **build**, Cluster Runtime behavioral analysis **Cluster config management** for clusters deploy and runtime Threat detection / incident response Policy-based governance **Compliance assessments Compliance policies**

DevSecOps Teams

Operations Teams



Google Cloud

Containerization and Isolation

- Minimize the impact of an attack by isolating running applications with
 - · SELinux & Security Context Constraints
 - Kubernetes namespaces (Projects), RBAC
 - Network Policies for microsegmentation
- Use resource quotas to prevent resource exhaustion
- Manage application access and protect application data
 - Single Sign On for user management
 - Secure routes / ingress, Red Hat Connectivity `link
 - Service mesh to encrypt pod-to-pod traffic
 - Egress IPs / firewall
- Monitor application metrics, logging and network communications
- Automate threat detection and response
 - Alert or kill pods based on anomalous behavior
 - Detect privilege escalation and risky processes such as cryptomining



Code, build, and monitor to a Trusted Software Supply Chain





Openshift on Google Cloud: Declarative Security



RED HAT Openshift Payments & Google Cloud Integration





By combining real-time AI, scalable infrastructure, advanced analytics, robust security, and collaborative innovation, a partnership with Google Cloud can be a game-changer for banks and payment service providers navigating the transition to Instant Payments and combating the rising tide of social engineering scams and approved push payment fraud



Legacy data architectures don't meet the needs of the Al era





of companies excel at maximizing value from data

Accenture 2023, Cloud Data Value

Legacy data platforms are hindering Al innovation



Economics

High TCO - hardware, maintenance & licensing

Complex data governance

Innovation



Limited in-built AI capabilities

Skills-gaps

No data democratization



Time to Value

Data silos

Process bottlenecks



If you are the First Step:

Partner with Google Cloud to benchmark your foundations for Al

The Data & AI benchmarking engagement results in deliverables that can position your team for immediate and future success on Google Cloud.





AI Hypercomputer

Flexible deployment and ecosystem partners

Partner ecosystem	Foundational mode	els Al21 labs	ANTHROP\C	co:here	contextual·ai	Mtferwe	osmo
	Systems integrator	accenture	BCG Deloitte	e. KPIMG	McKinsey & Company	🔛 quantiphi	tcs 66 degrees
	SaaS/application	BENDING SPOONS	∰DATADOG ⊋DataRobot	glean ∳GitLa	<u> </u> Jasper ab	salesfore () tabnine	UKG WRITER
	Infrastructure & platform	AIBLE	🔮 BROADCOM 🍓 Red Hat	⊓ NetA _l gretel	pp i «	Labelbox Invidia.	🥵 Snorkel





Thank you.

Google Cloud

