



Ravelin's Secure Growth Summit 2019

Gain insight into the fraud strategy and technologies
used by leading global online businesses

ravelin.com

Agenda

13 - 13.30	Refreshments, arrival of guests
13.35	The Bigger Picture: The Growing Cybercrime Economy
14.00 - 14.30	Just Eat - Globalising Fraud Practices to Balance Friction, Protection and Revenue.
14.30 - 15.00	BREAK
15.00 - 15.30	Machine Learning at Scale with Google Cloud.
15.30 - 16.00	eShopWorld - How to Enter Higher Risk Markets with Confidence
16.00 - 16.30	BREAK
16.30 - 17.00	Maximising Acceptance in a PSD2 World
17.00 - 17.45	Technology and the Analyst
17.45 - 18.00	Closing remarks
18.00 +	Drinks and Dinner



Ravelin's Secure Growth Summit 2019

Gain insight into the fraud strategy and technologies used by leading global online businesses

The background features a complex, abstract network of glowing lines and nodes in shades of blue, purple, and orange, set against a dark gradient. The lines form a dense, interconnected web, with some nodes highlighted in brighter colors.

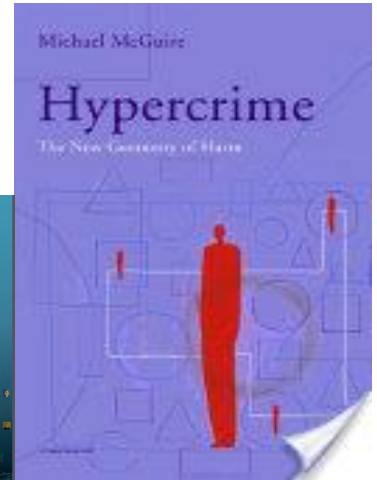
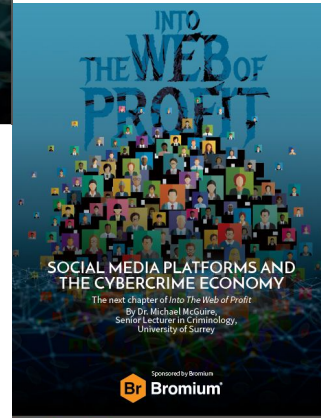
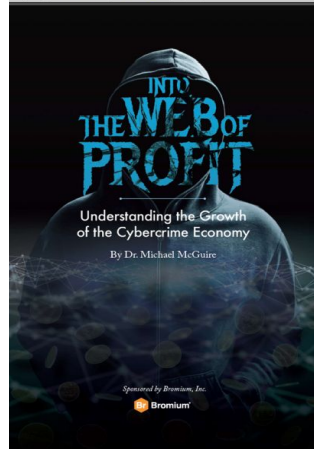
Into the Web of Profit:

Rethinking Cybercrime

Dr Michael McGuire
University of Surrey

Backgrounds

- About me
- Dr Michael McGuire
- Criminologist
- University of Surrey
- Critical Cybercrime theorist



Backgrounds

- Fraud & cybercrime – its significance
- I aim to explore some key trends here in the context of findings of a 18 month piece of research
- The Web of Profit project
- Associated reports:
 - (i) Platform Criminality and the Cybercrime Economy
 - (ii) Social Media Platforms and the Clear Net
 - (iii) Darknet Markets and Cybercrime Platforms

Backgrounds

- Web of Profit Project
- Initial brief: – to understand the outputs of cybercrime, not its inputs
- **Not what cybercriminals 'do'** - attack vectors, malware types, perpetrators, computer dependent v computer enabled crime variants, etc etc
- **Why cybercriminals 'do'** - Revenues, laundering, spending investments etc etc.

Changing Perceptions of Cybercrime

Signature finding:

- Previous ways of modelling cybercrime increasingly unsustainable
 - They have not offered successful responses
 - Offence prevalence continues to grow, offences become more varied and diverse
 - Continued disruption and financial loss to enterprise and almost every other sector of society as result
 - The capacity of law enforcement and policy makers to respond effectively remains limited
-
- We need to rethink what we think of as ‘cybercrime’

Once upon a time.....

- We thought `cybercrime' happened in a place called 'cyberspace'
- It was about 'technical' things like viruses or network compromises
- It involved clever young computer experts - hackers, crackers etc.
- It was about stealing credit card numbers, banking details etc.
- Enhancing cybersecurity (perimeter protection & firefighting) was the optimal response



The New Cybercrime

- But the research identified a **far wider** range of factors crucial to cybercrime as it is currently constituted

The New Cybercrime

- A dizzying range of methods & mechanisms for generating **revenues**, often at industrial scales

\$\$ Crimeware \$\$

\$\$ IP Theft \$\$

\$\$ Advertising \$\$

\$\$ Trade Secrets \$\$

\$\$ Counterfeits \$\$

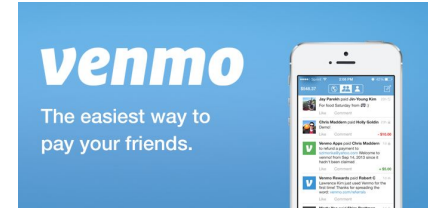
\$\$ Skills hire \$\$

\$\$ Data Trading \$\$

\$\$ Online Markets \$\$

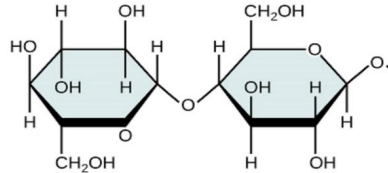
The New Cybercrime

- Rapidly expanding range of digital currencies and payment systems
- Some of which underpin cybercrime revenue generation



The New Cybercrime

- Specialised economic agents - such as producers, suppliers, service providers and consumers.
- A new form of raw material and trading commodity - the extraction and exchange of **data**.
- Not just data from stolen credit or debit cards
- A range of newer data forms with value :
 - hotel/airline loyalty points,
 - Netflix logins
 - 'likes' on Facebook
 - soft drink formulas
 - healthcare records



The New Cybercrime

- Specialised markets
- Tool supply, technical support and provision of skills and expertise
- Professionalisation and the development of career structures.
- Training, CVs, personal recommendations and references.

Dream Market
Ichudifyeqm4hdjj.onion
Established 2013

Drugs, Digital Goods, Hacking, Fraud,
Counterfeit, Electronics, Defense, Jewellery,
Software, Erotica, Data Leaks and so on!



The New Cybercrime

- Dedicated production zones and centres of income generation,
- EG 'Hackerville' fraud villages in Romania
- Troll factories in Moscow



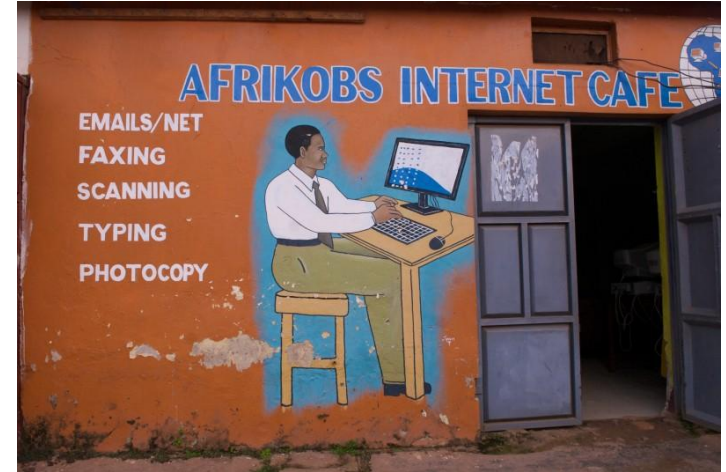
Râmnicu Vâlcea



Internet Research Agency
Savushkina Street, St. Petersburg

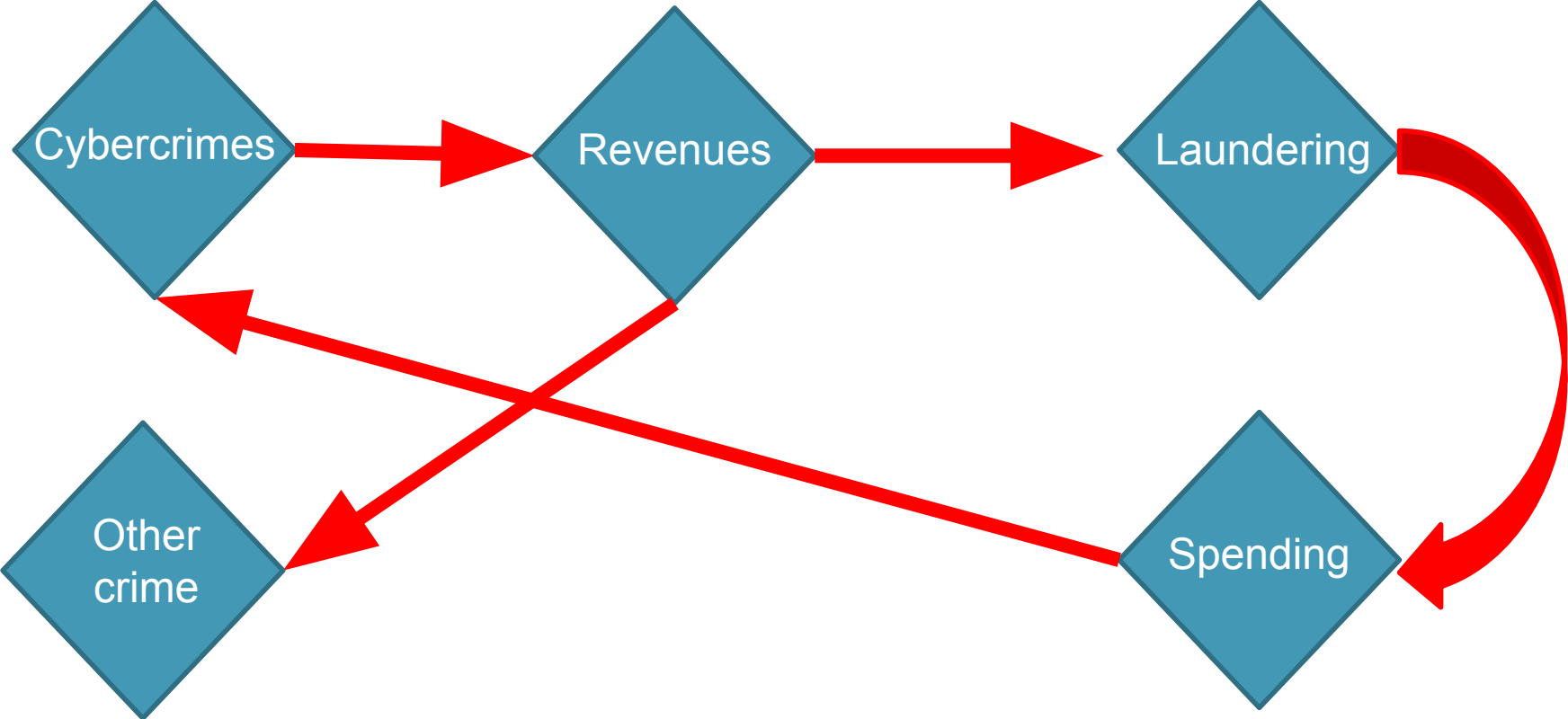
The New Cybercrime

- Romance fraud offices in Accra, Ghana



- Online counterfeiting centres in China/Vietnam/etc

A Cybercrime Economy



Cybercrime Revenues

Cybercrime Economy now worth:



\$1.5 trillion in revenues annually - at minimum

Cybercrime Revenues v Fortune 500 companies & Nation States

\$1.5 trillion compared to:

Walmart	\$485,873,000 <i>per annum</i>
Berkshire Hathaway	\$223,604,000 <i>per annum</i>
Apple	\$215,639,000 <i>per annum</i>
<hr/>	
Saudi Arabia	\$0.75tn
Portugal	\$0.2tn

The Cybercrime Economy – Revenue Generation

- Highest earners can make up to **\$2m/£1.4m** – almost as much as a FTSE250 CEO
- Mid-level operators can make up to **\$372,000/£263,000** – greater than the average for a US CFO
- Entry level hackers can make **\$30,000/£21,000** – on par with the average UK graduate income

The Cybercrime Economy – Revenue Generation

\$1.5 trillion dollars - break down:

Illicit/illegal online markets	\$860bn <i>per annum</i>
Trade Secret/IP theft	\$500bn <i>per annum</i>
Data Trading	\$160bn <i>per annum</i>
Crimeware/CaaS	\$1.6bn <i>per annum</i>
Ransomware	\$1bn <i>per annum</i>

Fraud

- A conservative estimate because many categories were not included/lacked sufficient data to calculate
- For example: Romance fraud
- In general, **fraud** at the centre of many of the categories used to calculate revenue generation.
- And many more where no calculation was possible
- Cybercrime has been characterised as ‘fraudinogenic’
- For example:

The Cybercrime Economy – the role of fraud

Illicit/illegal online markets

Fraudulent goods & counterfeiting

Trade Secret/IP theft

Spoofing, Impersonation, Sale of product designs

Data Trading

Card fraud, chargeback/friendly fraud

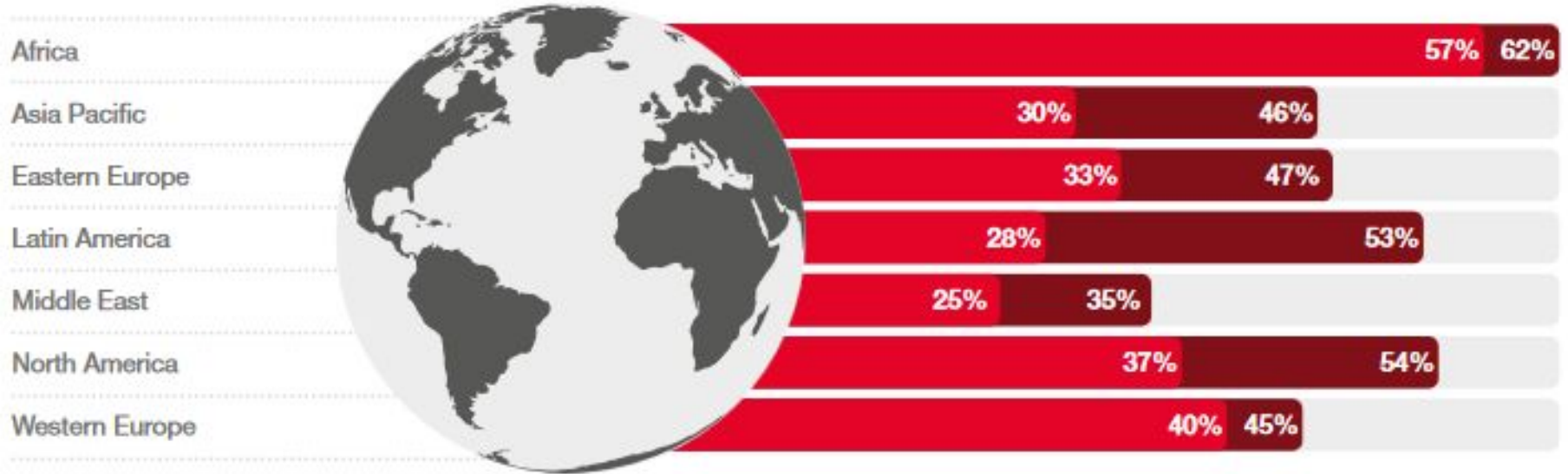
Crimeware/CaaS

Account takeovers, Identity theft

Fraud – some recent indicators

- Organizations lose up to **5%** of their annual revenues to fraud
- In 2018 **49%** of respondents to the Global Economic Crime and Fraud Survey said their companies had been victims of fraud or economic crime, up from **36%** in 2016
- But - only **54%** said they have conducted a fraud or cybercrime risk assessment in the past 2 years

Global rise in fraud/economic crime



■ Reported economic crime in 2018 ■ Reported economic crime in 2016

Fraud – some recent indicators

- Projected total global fraud losses amounted to nearly USD **\$4 trillion** in 2018
- E-commerce & card fraud significant components in this - Global Card Fraud alone projected to reach **\$50 billion** by 2025
- Consumer-perpetrated chargeback fraud, also known as “friendly fraud,” is reported to account for the largest share of those losses
- Merchants account for **29%** of global gross fraud losses (c\$6.7 billion) Card issuers around **70%**

Three misconceptions about cybercrime

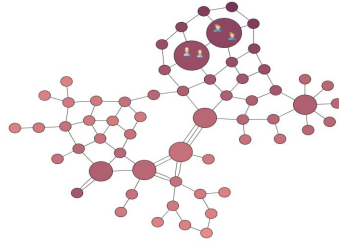
- One factor fuelling this growth are three misconceptions around cybercrime

Cybercrime perpetrators are opportunistic, young & work in small groups or alone

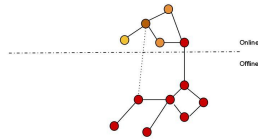
- Up to 80% of cybercrime activity now organised
- Over 45% of group associates aged 36 or above
- Most cybercrime groups (60%+) not temporary or ephemeral but associate with other for 1 year or longer
- Only 25% of cybercrime groups have a length of association < 6 months
- Cybercrime groups have a variety of different structures

SIX Types of Cybercrime groups

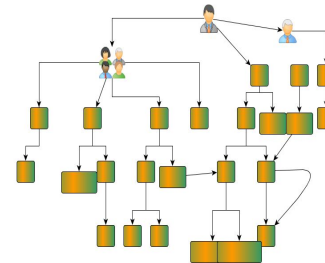
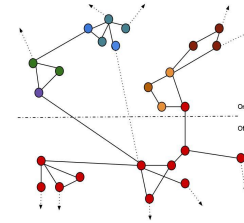
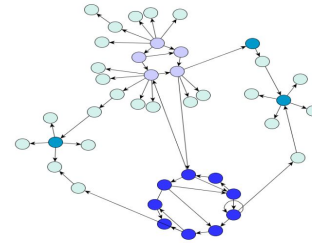
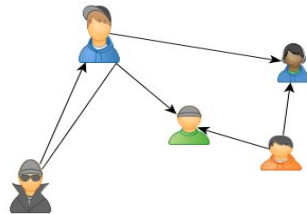
Type 1
Swarms & Hubs



Type 2
Hybrids



Type 3
Aggregates & Hierarchies



Economic Cybercrime/fraud is “victimless”

- Impacts can be mitigated for by banks, insurance or ‘write-offs’
- No-one is really ‘hurt’?..... BUT:
- Whilst around 55% of cybercriminals spent revenues on immediate needs (e.g. **paying their bills**) or **hedonistic** purchases – eg. **buying drugs, paying prostitutes, expensive jewellery or sports cars etc**
- **30%** of cybercriminals invested revenues– e.g in **property** or **financial instruments**
- **20%** of cybercriminals spend at least some of their revenues of reinvestments in further criminal activities - some serious like trafficking or terrorism

Cybercrime like a 'business' ?

- Early views of cybercrime were flawed, centring too exclusively upon its tools - its 'technological' character
- Socio-economic aspects of cybercrime have begun to be recognised
- But one such idea - that 'cybercrime is like a business' is also fatally flawed
- It causes us to overlook the vast, complex and hyperconnected nature of contemporary cybercrime
- As the Web of Profit research suggested - the cybercrime **economy** is far more appropriate metaphor
- The failure to recognise this permits the cybercrime economy to become increasingly blurred with the legitimate economy
- In turn, this raises prospect of a variety of long term societal harms

Cybercrime economy, the legitimate economy & harm

(1) Legitimate business & law abiding citizens being sucked into the wake of this economy:

- EG: In 2017, Western Union ordered to pay \$586m by DoJ as a result \$632 million being unwittingly transferred in relation to online lottery scams, romance frauds & 419 scams
- Growth of quasi-legal darknet traders (drugs, crimeware, etc)
- Increasing temptations for young people to act as money mules

(2) Global trading becoming distorted and vulnerable to corruption:

- EG - money laundering
- UN estimates 1.7 – 2% of Global economy (Up to \$2 tn) being laundered
- Cybercrime revenues fundamental to this
-

Protection as a civic duty

- All this emphasises the value of adequate network protection
- Not just a company need – a civic, societal duty
- Losses which are ‘written off’ do not disappear into the ether
- They help fuel the vast and growing cybercrime economy
- Which in turn fuels:
 - Further cybercrime
 - Organised crime
 - Serious crime like people trafficking, terrorism, arms trading etc
- Legitimate business and law abiding citizens engaging in quasi-legal behaviours as a result of becoming absorbed by the vast cybercrime economy.



Thank you.

Dr Michael McGuire
University of Surrey

Agenda

13 - 13.30	Refreshments, arrival of guests
13.35	The Bigger Picture: The Growing Cybercrime Economy
14.00 - 14.30	Just Eat - Globalising Fraud Practices to Balance Friction, Protection and Revenue.
14.30 - 15.00	BREAK
15.00 - 15.30	Machine Learning at Scale with Google Cloud.
15.30 - 16.00	eShopWorld - How to Enter Higher Risk Markets with Confidence
16.00 - 16.30	BREAK
16.30 - 17.00	Maximising Acceptance in a PSD2 World
17.00 - 17.45	Technology and the Analyst
17.45 - 18.00	Closing remarks
18.00 +	Drinks and Dinner



Ravelin's Secure Growth Summit 2019

Gain insight into the fraud strategy and technologies used by leading global online businesses

JUST EAT

*The Journey to Globalising Fraud Practices to
Balance Friction, Protection and Revenue*

RAVCON, May 2019

Who are we?

Ben Shipway

Head of Product & Technology
- FinTech -

Lora Walsh

Global Fraud Manager
- FinTech -

Just Eat



Our vision

*Serving the world's greatest
menu. Brilliantly*



Hello, we're Just Eat

We operate a leading global hybrid marketplace for online food delivery, providing Customers with an easy and secure way to order and pay for food from our Restaurant Partners.

100k+

Restaurant Partners

100

cuisine types

26m+

Active customers

3,600+

Just Eat team



Tech at Just Eat

600+ people in Tech

26m+ active customers

35+ teams

450+ services

7 orders a second

2,500+ orders/min at peak times

1.6M+ metrics/min

1.5TB+ logs/day

500+ releases/week

43% Revenue Growth (FY18)



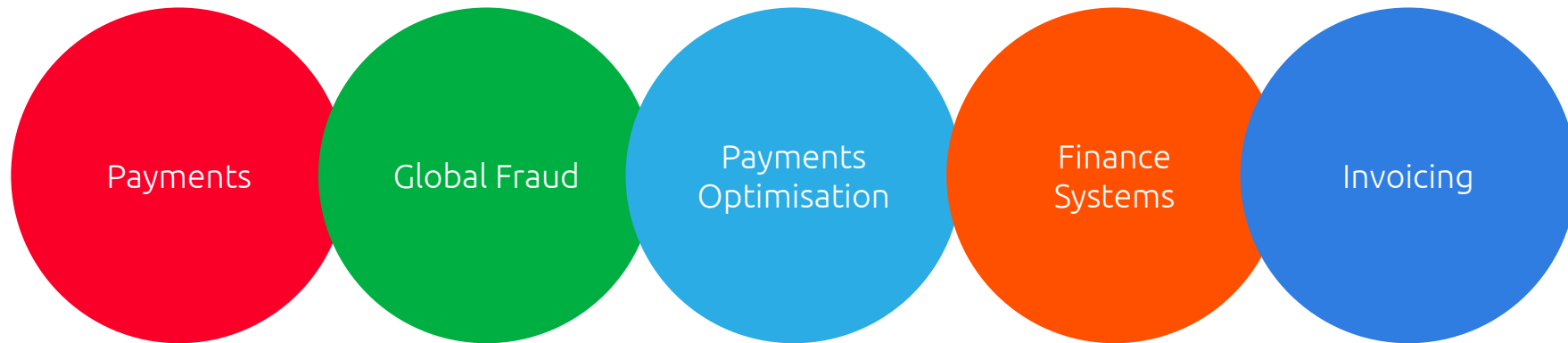
JUST EAT

FinTech

Providing an end to end payment acceptance capability, with dynamic payment flows and routing, adding value for our customers and maximising commerciality

Who are FinTech?

Product and operations working together to provide the best payments and finance capability available



“Make paying for a takeaway quick, easy and painless for all our customers”

“Protecting our customers and restaurants against fraud through best practice and best in class fraud tools”

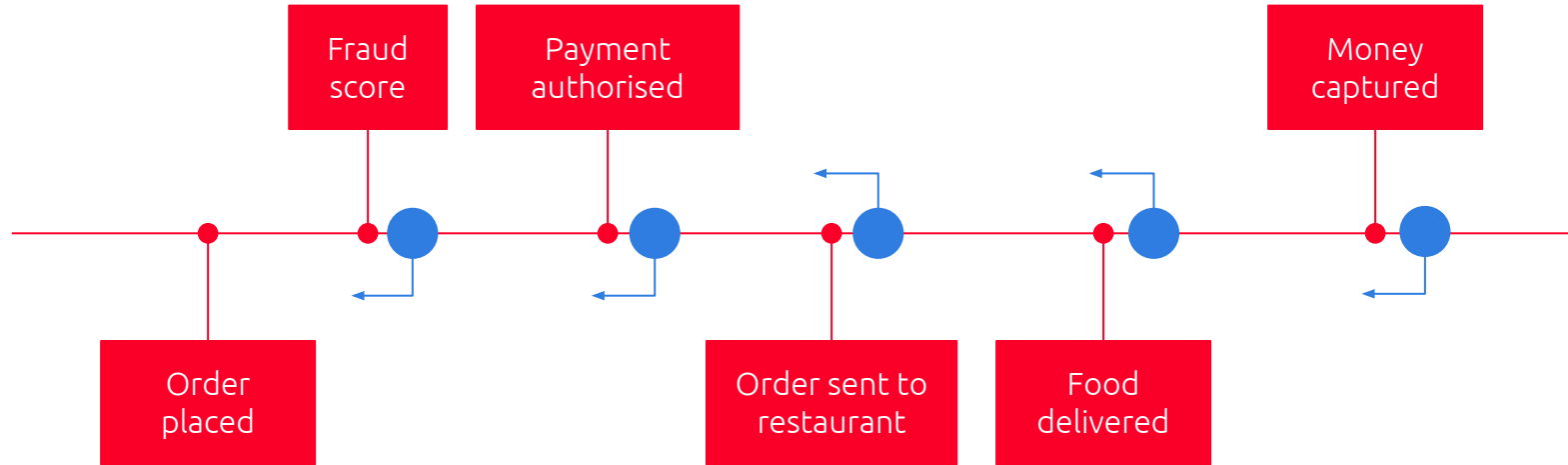
“Maximising transaction acceptance rates at the lowest possible cost”

“Ensuring the reliability, flexibility and integrity of our finance systems”

“Paying our partners the right amount, at the right time, every time”

The Problem

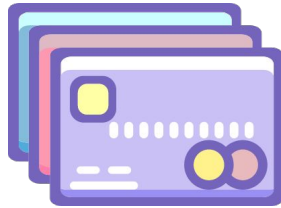
A typical order



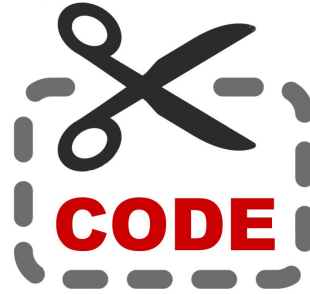
The Present

The Fraud Problem

Ecommerce



Vouchers



Process



Cash







Gift Cards



The Past

The Approach

Inconsistent global approach to tackling fraud with Segregated tooling, teams and processes:

-  Focus on chargeback cost reduction
-  Blanket approach to 3DS
-  Reactive and regressive
-  Limited data to understand impact

People

Inconsistent global approach to tackling fraud with Segregated tooling, teams and processes:



Specialised fraud team for UK market



Outsourced manual review team for AU market



Customer care teams managing blacklisting



AdHoc support given to by UK team in 'emergencies'

Tools and Processes

Inconsistent global approach to tackling fraud with Segregated tooling, teams and processes:



Manual resource intensive processes



Four fraud tools; some pre-auth, some post-auth



Questionable chargeback disputing process



Rules based tooling

The Result

Inconsistent global approach to tackling fraud with Segregated tooling, teams and processes:

1

Different capabilities per market

2

Inconsistent rules and processes

3

Expensive tooling costs

4

Resource mismanagement

5

Delayed response to fraud issues

The Present

Fraud Approach

A new vision

- Understanding and support the different needs of our markets
- Revenue Balance as main driver
- Dynamic risk routing
- Automation/streamlining
- Data informed

Why globalise?

The need for a redesign

- A move to more centralised fraud management
- Increased internal focus on fraud
- Lack of expertise in countries to manage growing risk
- Tooling not sophisticated enough to support business size
- Opportunity to leverage global volumes
- Opportunity to leverage expertise knowledge

Globalisation Approach

- Centralising people, tools and processes
- Separating out fraud and payment optimisation
- Move from finance into tech
- Focus on revenue balance

Globalisation Process

The journey bringing together countries

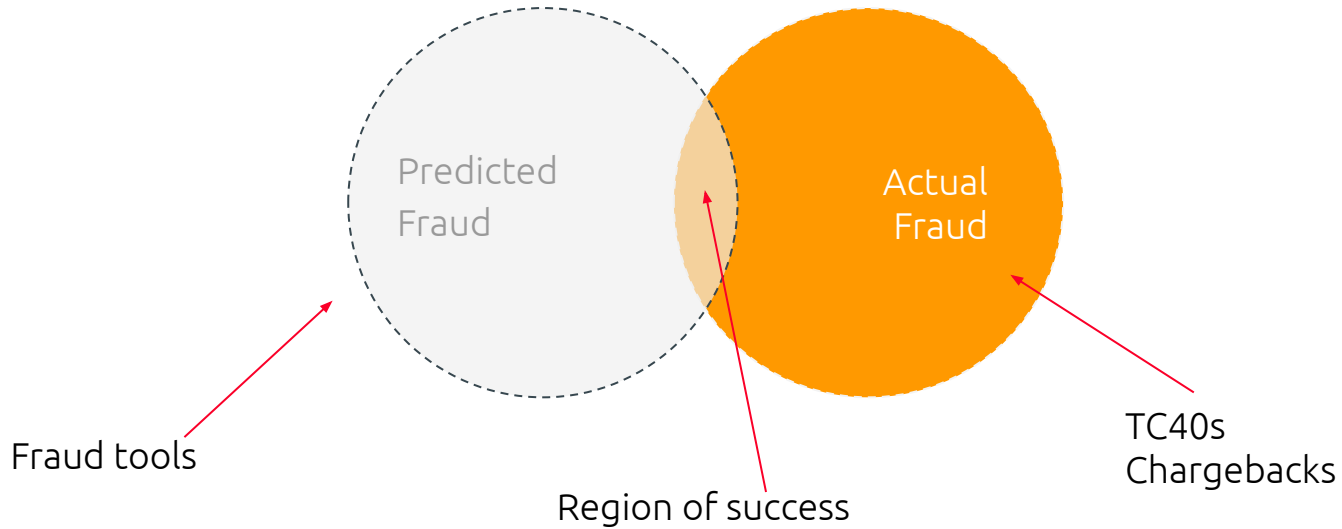
- Country by country review of practises to find opportunities
- Propose gains / prove value with existing tooling
- Gain confidence of local markets to get buy in
- Restructure

Problems solved

- Apprehension from markets
- Lack of fraud education
- Limited resource
- Varied tooling

Measuring Success

Centralising risk tooling



KPIs measured:

- Expected 3DS rate
- Expected block rate
- Fraud detection rate
- False positives rates



Ravelin

About

- Ravelin are subject matter experts in on-demand fraud
- They are a flexible startup
- Machine learning technology very responsive to fraud attacks (compared to rules)

Tailored offering

- Built a restaurant fraud portal for managing restaurant fraud.
- Built a bespoke CC portal for looking up transactions
- Ability to handle cash, voucher and credit transactions

ethoca™

- Agreed global contract & expanded use to more markets
- Used to avoid CB fee
- Used for blacklisting
- Gives early visibility on fraud & fraud spikes
- From 2018 > 2019, an increase of x4 cost saving

Global Process

A common way of working

- Blacklisting
- Restaurant Fraud Monitoring
- Proactive investigations
- Reporting

Global Team

Working smarter

- Automation
 - Reporting, blacklisting, etc.
- Upskill team
 - SQL, BigQuery, Tableau
- Workload management
 - Jira
 - Support from local markets
- Globalised tools and processes
 - Centralised tools to manage
 - Standardised processes



Card:

	<i>UK</i>	<i>ANZ</i>	<i>ES</i>	<i>IE</i>	<i>IT</i>	<i>DK</i>	<i>NO</i>
3DS impact →	-67%	0 > 5%	-90%	-79%	-89%	0 > 2%	0 > 2%
Block rate impact →	-48%	-55%	-42%	-73%	-72%	-46%	-55%
Reduction in fraud chargebacks →	-74%	-67%	-44%	+15%	+21%	-60%	-58%

Cash:

- Also live on cash orders in the UK
- Reduced cash fraud losses by 15%

The Future

The Approach

1

Push the problem upstream

2

Automation, automation, automation

3

Holistic KPI Management

4

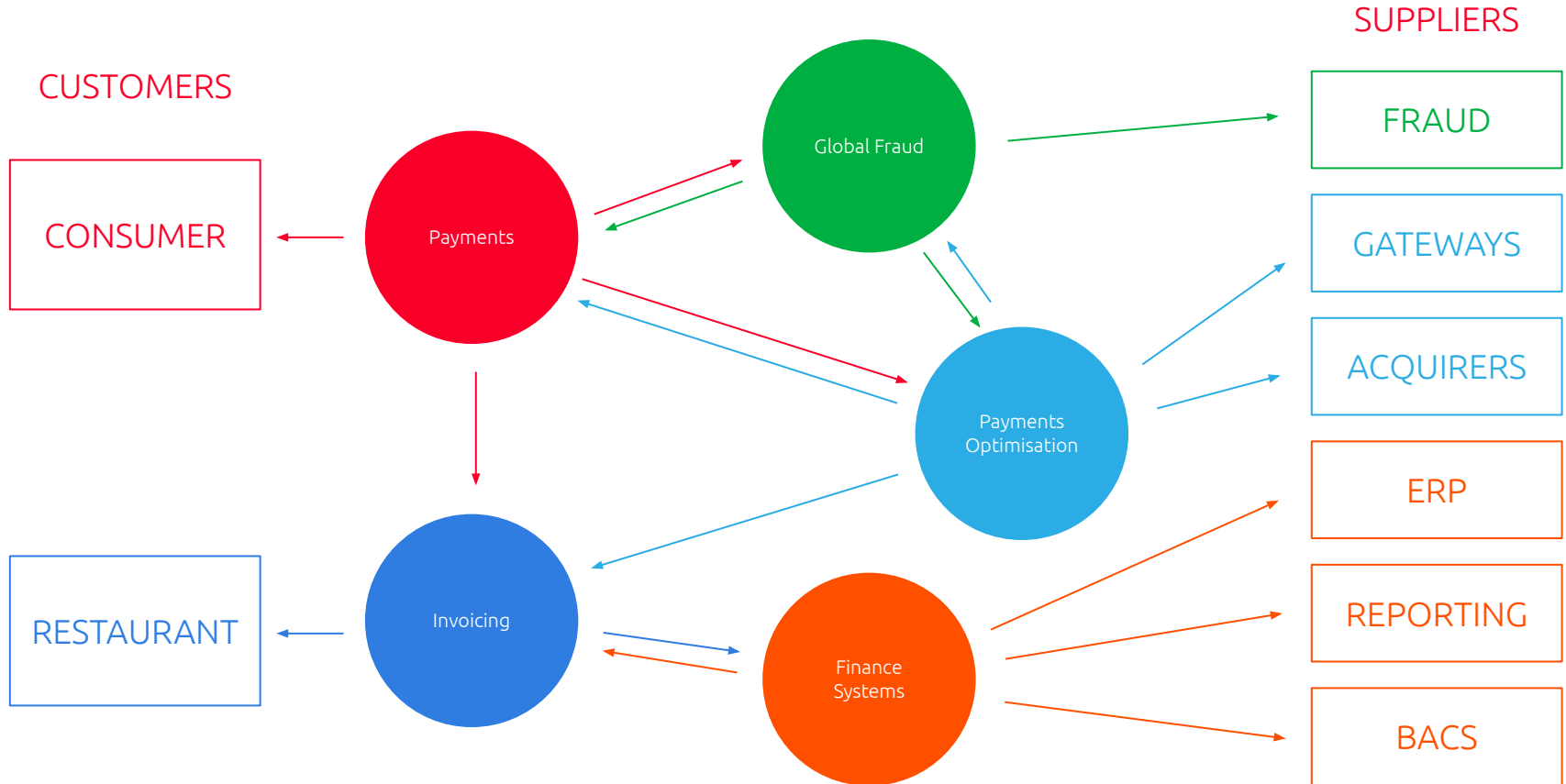
Capability Measurement

5

An enabled team

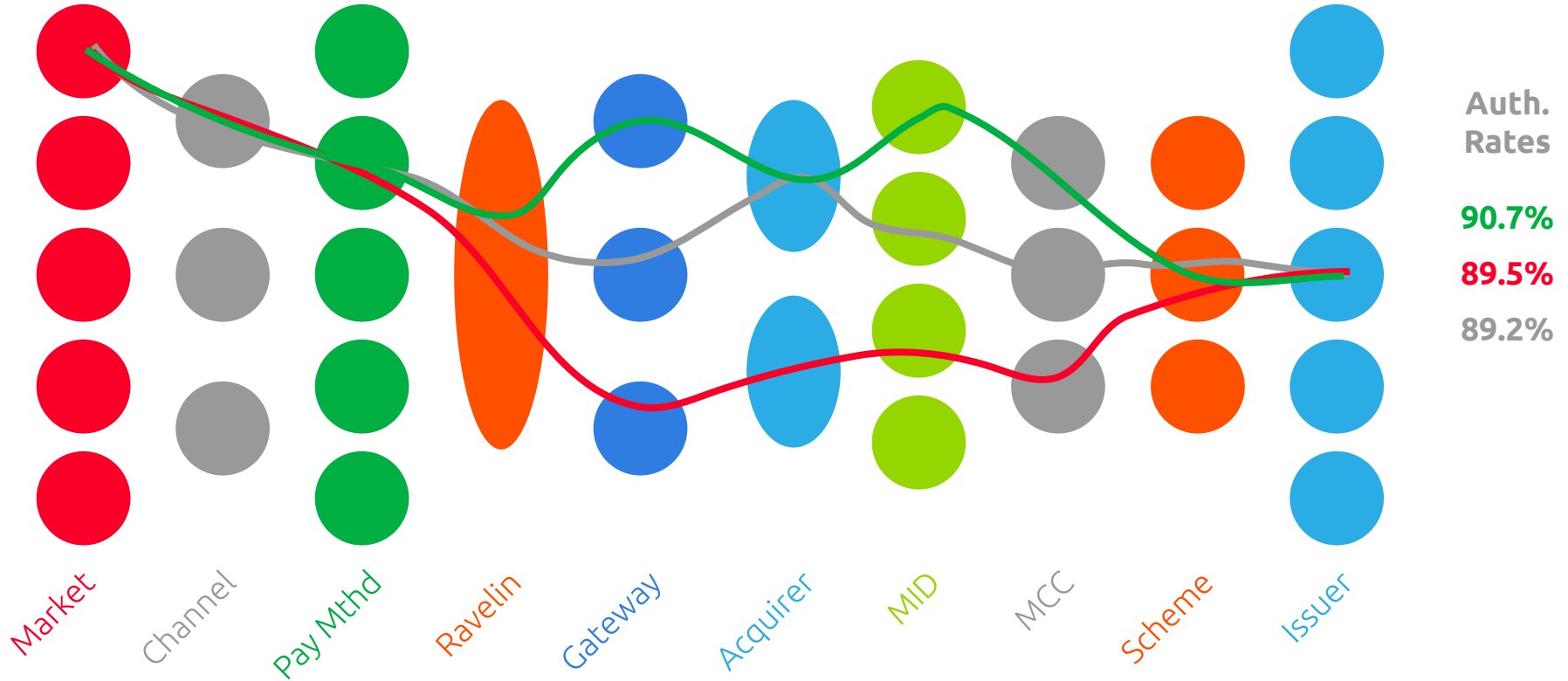
A Combined Capability

Decisions and changes affect KPIs, operational metrics and costs across the whole payment capability



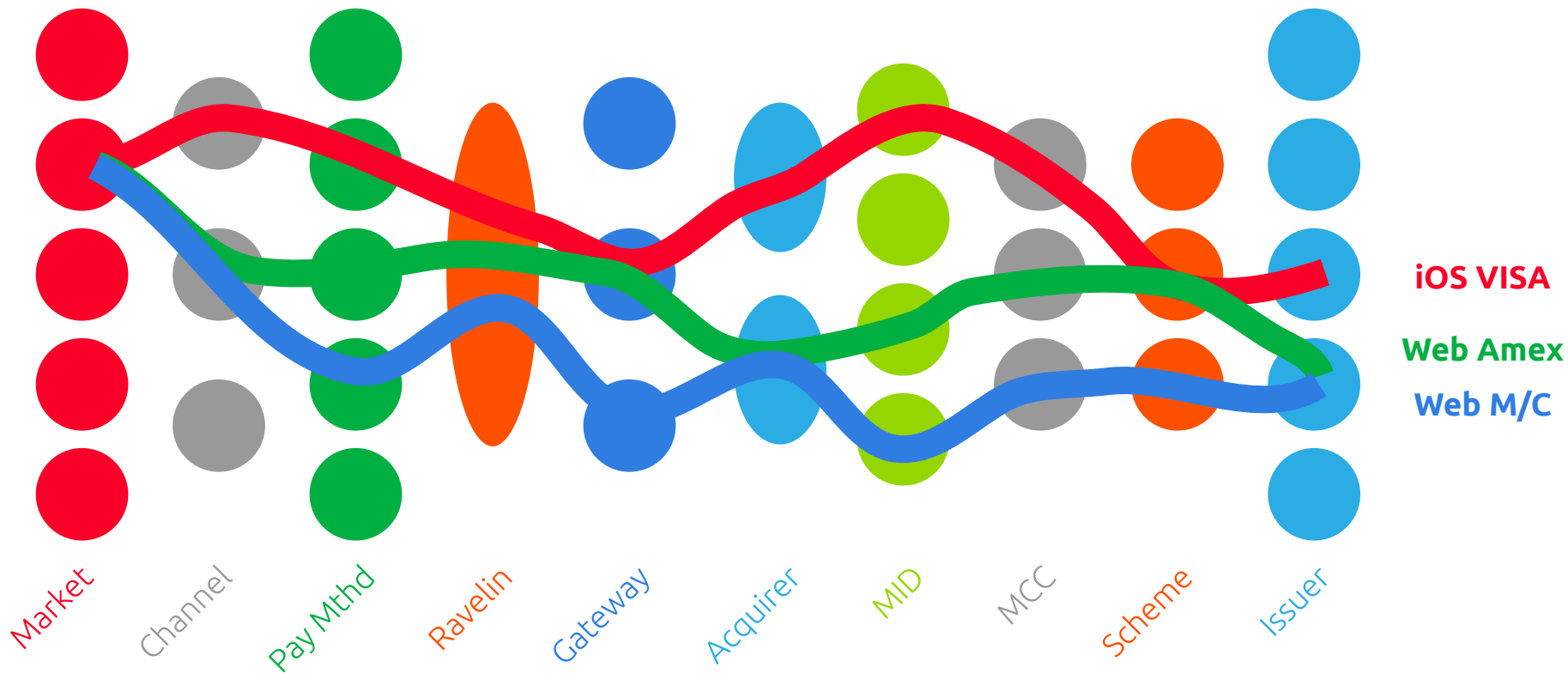
A Combined Capability

A single transaction routed three different ways can have very different acceptance rates



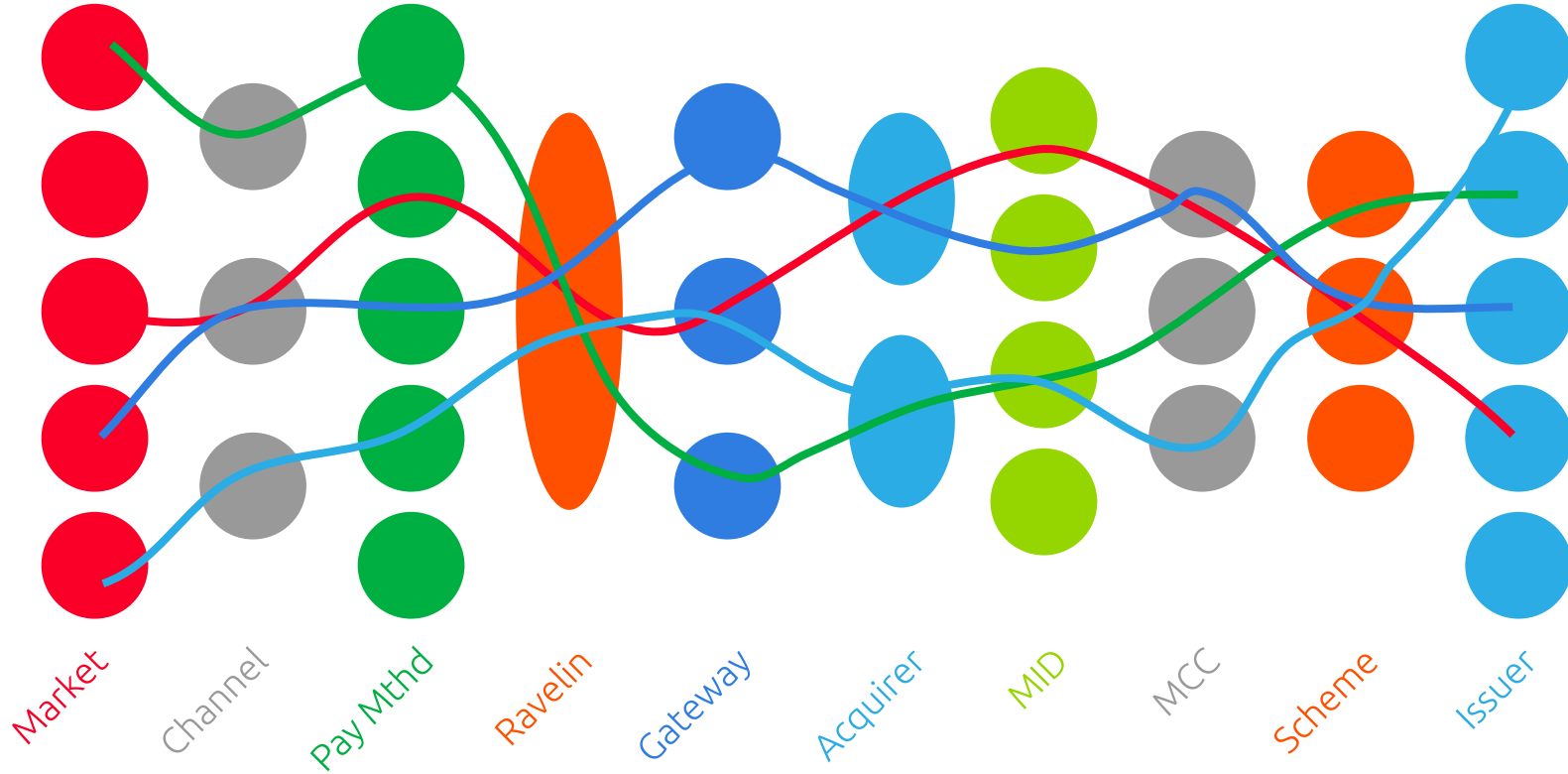
A Combined Capability

Transaction routing based on bandings, learnt over time, to produce the best rates for certain transaction cohorts



A Combined Capability

Dynamic real-time routing of individual transactions, balancing both learned auth rate bandings and KPI management



Implementation Pipeline

1

Fraud as a first class global capability

2

Automation of dispute management

3

Cash fraud

4

Ravelin rollout

5

Dynamic MCC routing

5

Offline payments

The take aways

The take aways

1

Combined technology and fraud strategy

2

Best in class tooling

3

Agile and collaborative partnerships

4

Think big, not small

Thank you

Ravelin's Secure Growth Summit 2019



Refreshment Break

See you soon

ravelin.com



Refreshment Break

Welcome back




Google AI at Scale

RavCon May 2019

Charlotte Pindar, Customer Engineering

Google Cloud





There will be
163 zettabytes
of data by 2025

- IDC, 2017

If your company
isn't good at
analytics, it's not
ready for AI.

- Harvard Business Review, 2017

62%

of people expect brands to deliver a consistent experience, but only

42%

think they do.

Google/Greenberg Survey, 2017

So many 'data silos'...



57%

**of marketers say
it's difficult to give
stakeholders in
different functions
access to data
& insights**

Forrester, July 2015

It's time
for a **new**
approach

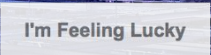


The Google logo is centered in the upper half of the image, rendered in its characteristic multi-colored font. The background is a vast, dimly lit server room with a complex network of metal beams and glowing server racks.

Google

A white, horizontal search bar is positioned in the center of the image. It is empty and features a small microphone icon on the right side, indicating voice search functionality.A rectangular button with the text "Google Search" is located below the search bar. The text is in a dark, sans-serif font.

Google Search

A rectangular button with the text "I'm Feeling Lucky" is located to the right of the "Google Search" button. The text is in a dark, sans-serif font.

I'm Feeling Lucky

A wide-angle, high-angle shot of a massive server room. The room is filled with rows of server racks, each illuminated with a soft blue glow. The ceiling is a complex, industrial-looking structure of metal beams and pipes, with several long, rectangular light fixtures hanging from it. The floor is a light-colored, polished surface. The overall atmosphere is one of a high-tech, industrial environment.

**“So what,
I’m not Google”**

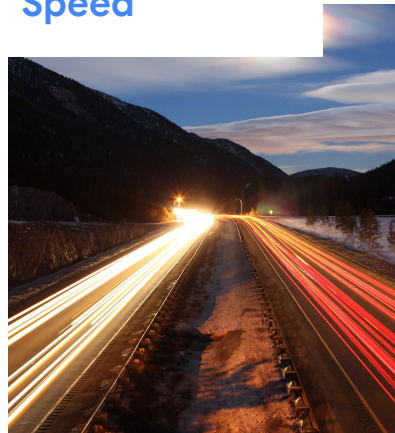
Why Google Cloud

Scale



Instant access to thousands of machines with Google Cloud

Speed



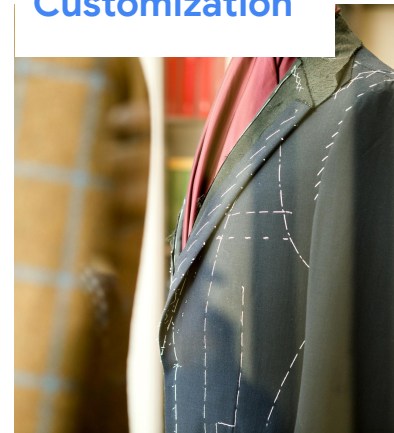
Stay ahead of the competition, and be more agile.

Quality

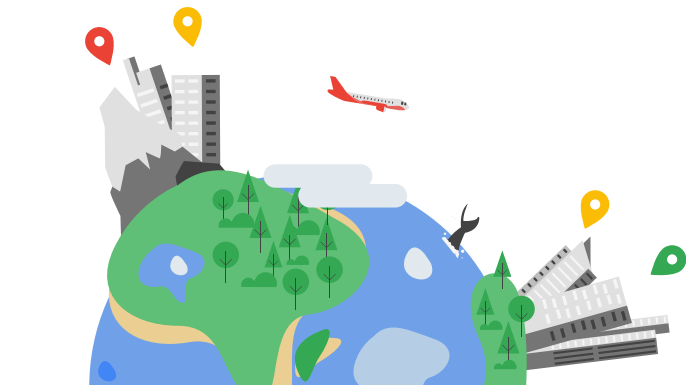


Be more data driven and use pre-trained highly accurate AI models to solve business needs

Customization



Easy to customize ML models with Google domain expertise and Advanced Solutions Lab



Google's mission

Organize the world's information and make it universally accessible and useful



Google Cloud

Enabling enterprises to collect, organize and use data

Google's AI Journey

A wide-angle photograph of a Martian landscape. The terrain is a mix of reddish-brown sand and rocky ground. In the center, a winding, dark-colored path or channel cuts through the landscape. The background shows a vast, flat expanse of the planet under a hazy, orange-tinted sky. The overall scene is desolate and barren.

“...it’s time to get Googley”

If everyone spoke to their phone for 3 minutes, we’d exhaust all available computing resources

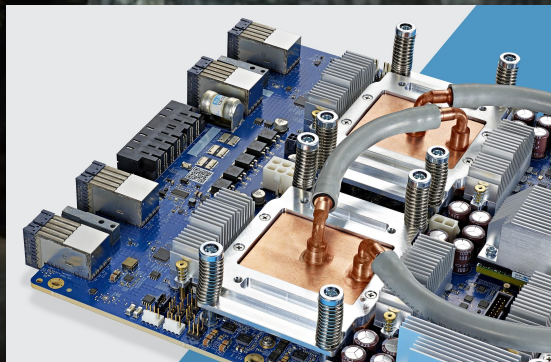
-- Jeff Dean, 2014



Hi, how can I help?

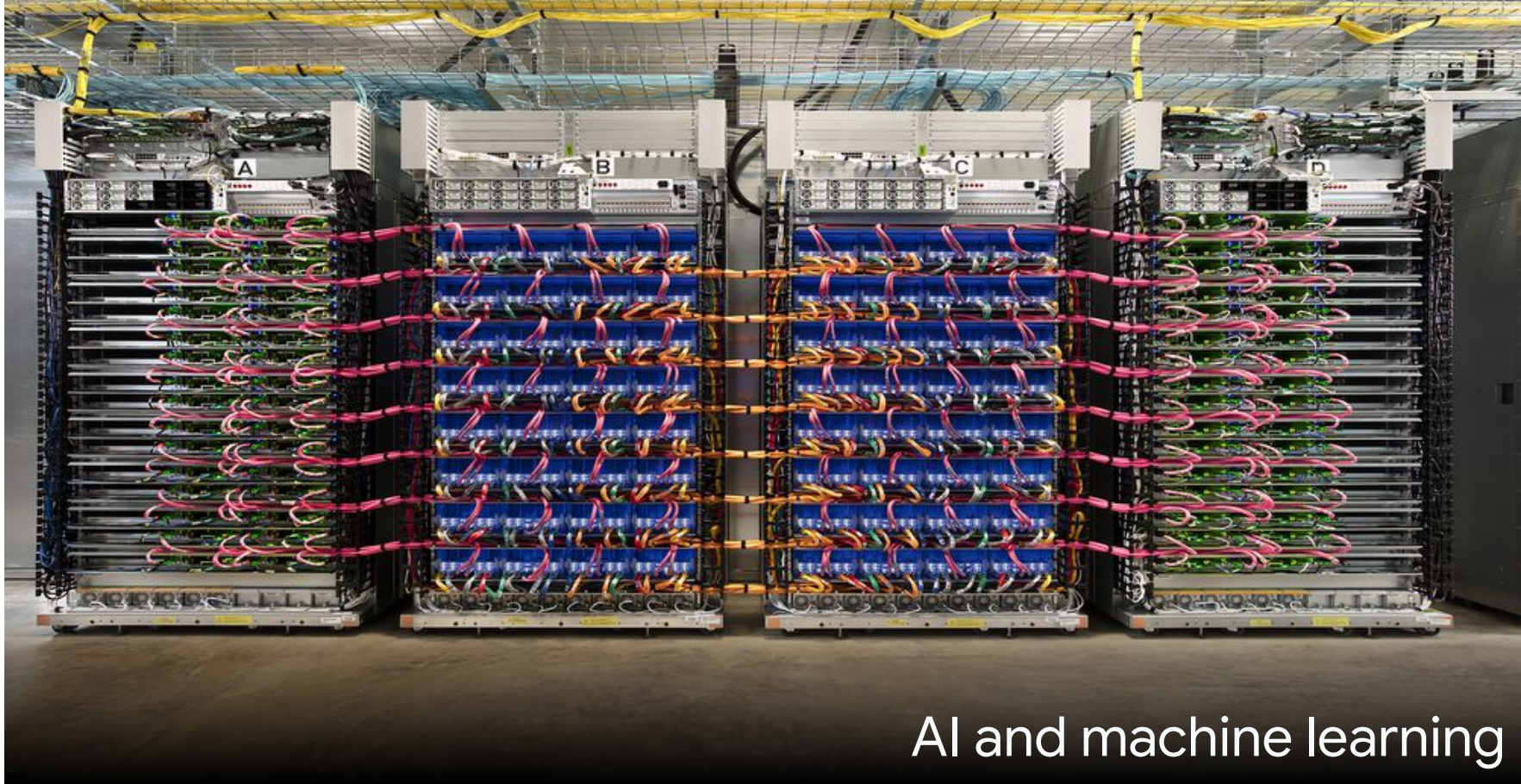
None

PS3.0



GPUs

Researchers began to notice that neural network mathematics closely resembled the algorithms to shade pixels in graphics cards (GPUs).



AI and machine learning



AI and machine learning

Where is Google Cloud helping Retailers?

Faster insights with data

Predictions with AI

Dynamic customer experiences

Workforce transformation

Retail partners

IT agility

John Lewis

JUST EAT

Walgreens

FINISH LINE

TP Travis Perkins

THE HOME DEPOT
LUSH FRESH HANDMADE COSMETICS



oocado

ebay

verizon[✓]

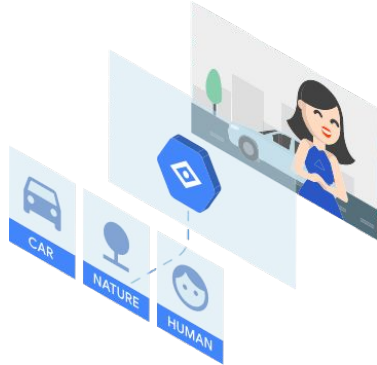
OVS



ALLSAINTS

LUSH

FRESH HANDMADE COSMETICS





AA-B97 WP3A

AA-C44 SP1

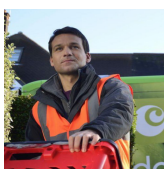
AA-A48 SP1

AA-A15 WP1

AA-F35

ocado
SMART PLATFORM

CREATED IN BRITAIN



INTUITIVE
EFFICIENT
CONVENIENT

AUTOMATION AND ROBOTS

MACHINE LEARNING

MOBILE APPS

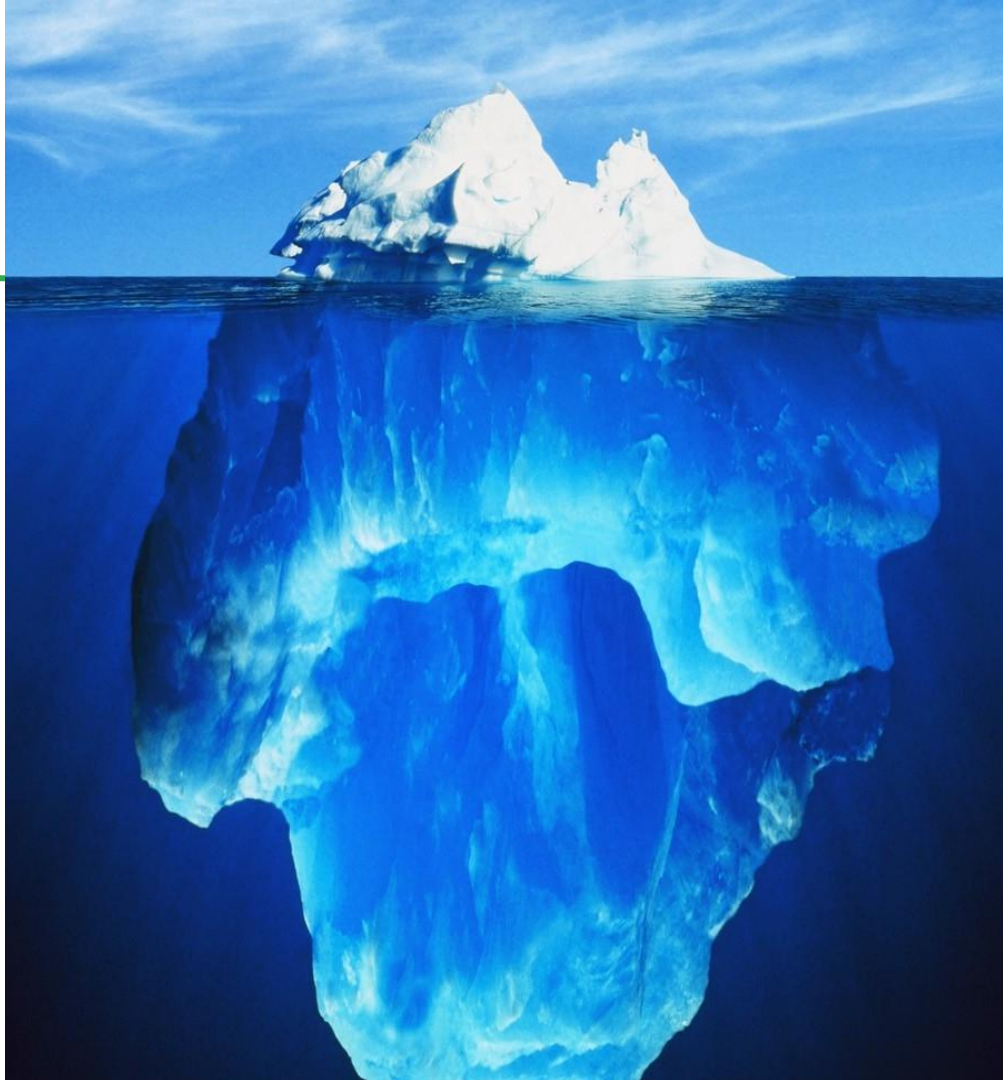
ROUTING SYSTEMS

DATA SCIENCE

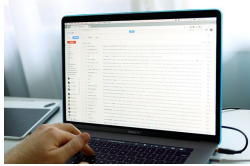
CLOUD

VISION SYSTEMS

SIMULATION



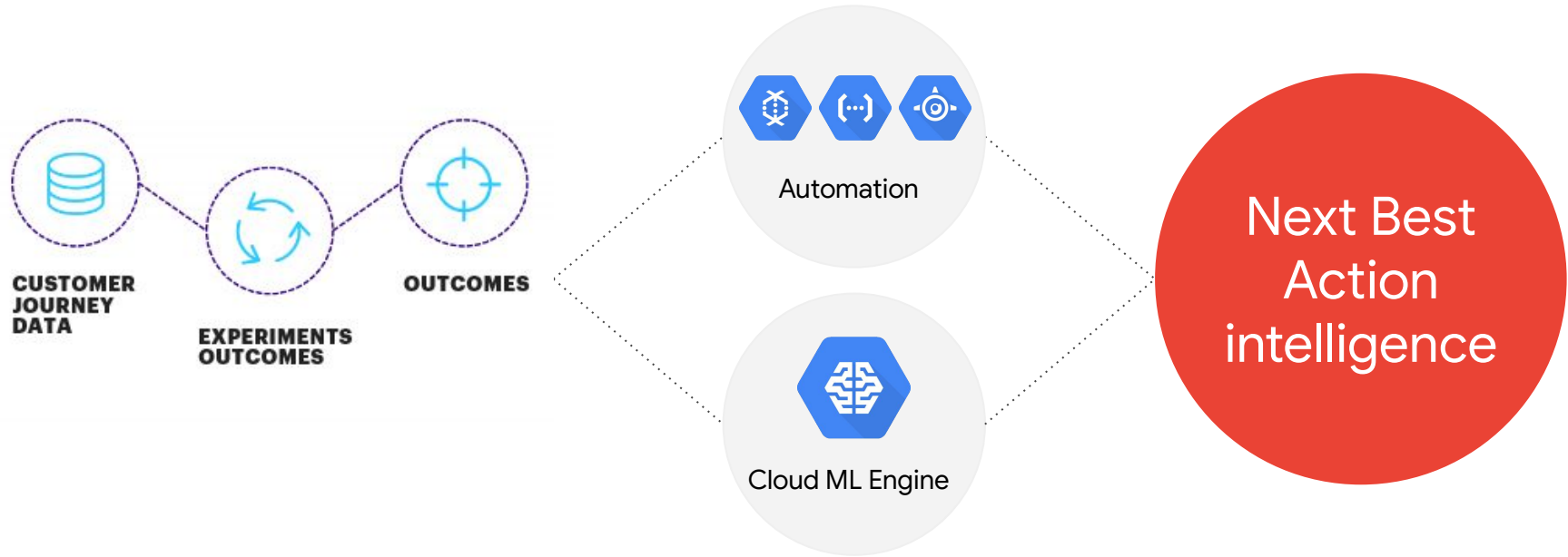
Prioritise urgent customer emails



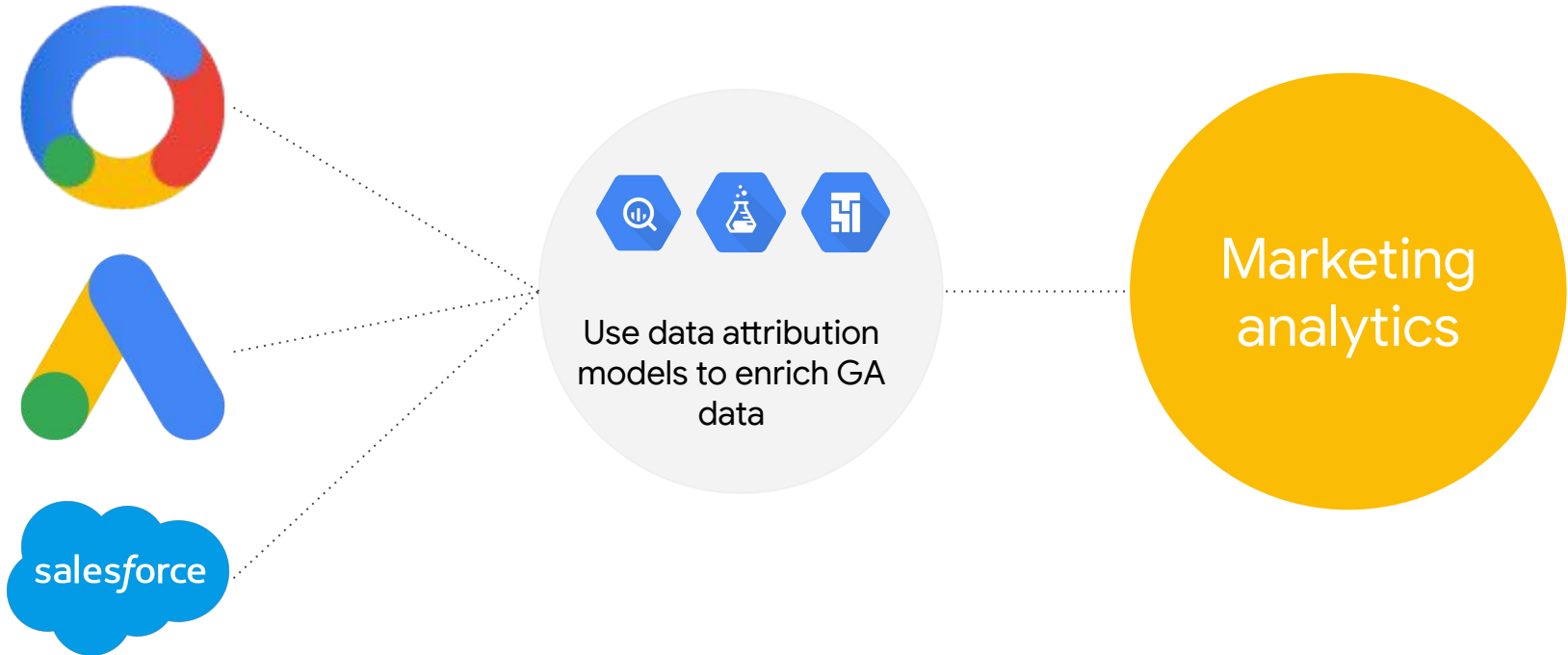
Sentiment
analysis and
entity
extraction

Unstructured
content
understanding

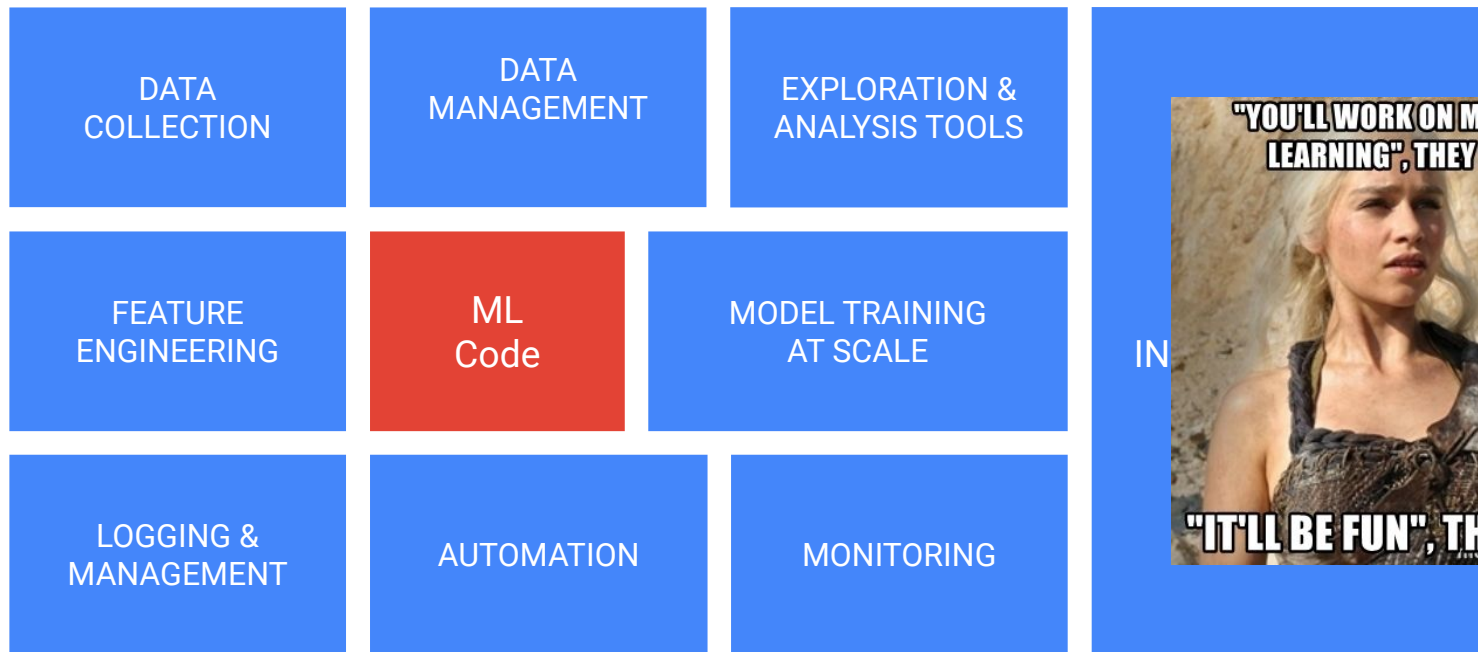
Customer retention



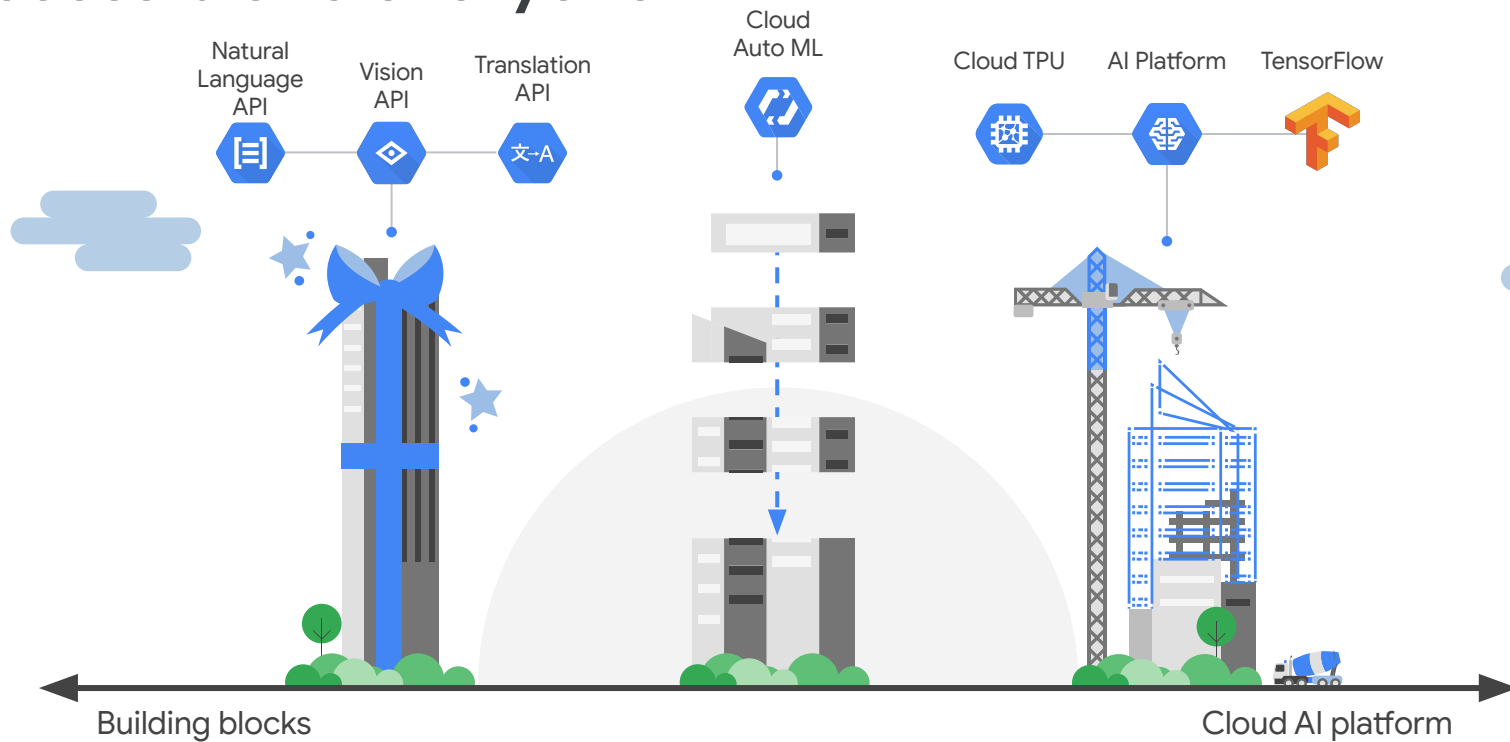
Using the cloud to join marketing data



This is what you need for production ML



Accessible to everyone





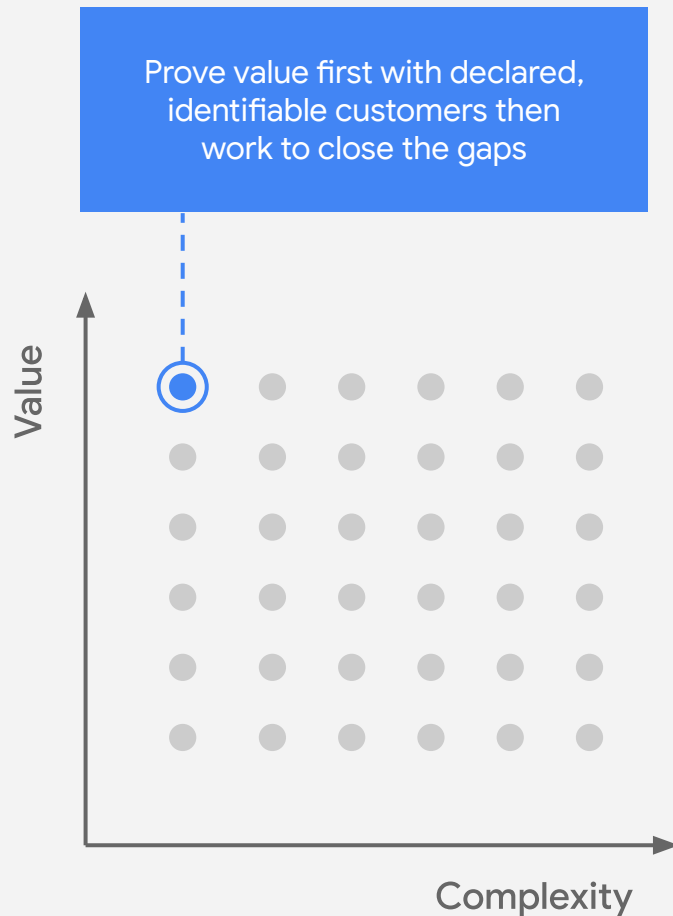
An open & secure platform



An open & secure platform

Bring in data
with a few clicks

Start with a simple but **high value use case**, expand from there





Thank you
cpindar@google.com

Agenda

13 - 13.30	Refreshments, arrival of guests
13.35	The Bigger Picture: The Growing Cybercrime Economy
14.00 - 14.30	Just Eat - Globalising Fraud Practices to Balance Friction, Protection and Revenue.
14.30 - 15.00	BREAK
15.00 - 15.30	Machine Learning at Scale with Google Cloud.
15.30 - 16.00	eShopWorld - How to Enter Higher Risk Markets with Confidence
16.00 - 16.30	BREAK
16.30 - 17.00	Maximising Acceptance in a PSD2 World
17.00 - 17.45	Technology and the Analyst
17.45 - 18.00	Closing remarks
18.00 +	Drinks and Dinner



Ravelin's Secure Growth Summit 2019

Gain insight into the fraud strategy and technologies used by leading global online businesses

ENTERING GLOBAL MARKETS AT SCALE



SELL GLOBAL. FEEL LOCAL.™

eshopworld

HELLO!

David Power

CSO eShopWorld



QUIETLY MAKING NOISE

- **Ranked #1 in 2015, 2016, 2017**
Deloitte Fast 50 Fastest Growing Tech Firms
- **Technology Exporter of the Year 2016, 2017**
Export Industry Awards
- **Technology Company of the Year 2017**
Software Industry Awards



THE GLOBAL OPPORTUNITY

“Crossborder B2C eCommerce sales will account for 20% of all eCommerce revenue by 2022, with 46% of consumers shopping across borders.”

Forrester Research

“Shoppers are more global than ever, and not content to settle for products only available in their home countries.”

eMarketer

ESHOPWORLD - A SNAPSHOT



\$650m+

Gross Merchandise Value (GMV) to be transacted in 2019

200+

Number of supported markets

25+

Number of global carriers

40+

Number of supported payment methods

ESHOPWORLD CROSSBORDER ECOMMERCE

Elegant solutions are often built on **complex foundations**.

Delivering outstanding customer experiences across **multiple global markets**.

The **best brands in the world** trust eShopWorld to reduce the complexity of selling across borders



PLATFORM

Cloudscale Technology

Localised Pricing

Optimised Payments & Fraud

Multiple webstores & Inventory

Global Hubs / Logistics

BENEFITS

Expert tools and guidance

Cost savings

Synergies and Economies of Scale

Speed to market

Efficiency and effectiveness

CALM ON THE SURFACE

SELL GLOBAL. FEEL LOCAL.™

eshopworld

GLOBAL DATA INFRASTRUCTURE

2014

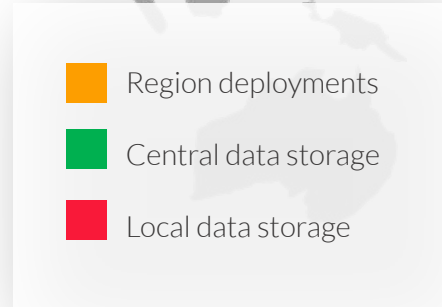


SELL GLOBAL. FEEL LOCAL.™

eshopworld

GLOBAL DATA INFRASTRUCTURE

2019



SELL GLOBAL. FEEL LOCAL.™

eshopworld

GLOBAL INFRASTRUCTURE



SELL GLOBAL. FEEL LOCAL.™

eshopworld

THE PRODUCT...*TODAY*

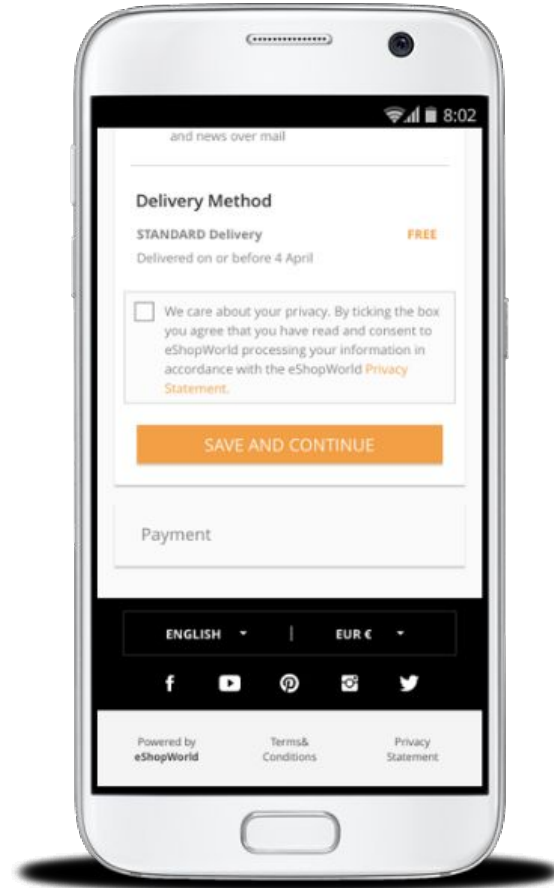
Pricing presentation

Frictionless, hosted checkout

Easy-peasy payments

Advanced fraud screening

Global & local acquiring



DO WHATEVER IT TAKES



SELL GLOBAL. FEEL LOCAL.™

eshopworld

**JOURNEY TO SUCCESS
IS BETTER SHARED**



THANK YOU



SELL GLOBAL. FEEL LOCAL.™

eshopworld

Ravelin's Secure Growth Summit 2019



Refreshment Break

See you soon

ravelin.com

Ravelin's Secure Growth Summit 2019



Refreshment Break

Welcome back

ravelin.com



Maximising Acceptance in a PSD2 World

Martin Sweeney



Liability vs Usability

Rock: Fraud

Hard place: 3D Secure



Liability + Usability
= Opportunity



Know thy enemy

Aussie Black Beard
@AussieBlacBeard

Follow

This verified by visa bullshit is doing my fucken head in!

10:11 AM - 4 Mar 2019

3 Likes



Retweet 3

Disgruntled Mage
@tyndyll



Follow

There's a special place in hell for whomever came up with Verified By Visa

LIKES

9



3:09 PM - 16 Sep 2016

Retweet 8

Alex Baxter
@lxbxr



Follow

Well Dell that's another sale lost due to Verified by Visa. In a way it's a good security system since it stops you from buying stuff.

8:05 PM - 15 Sep 2016

Retweet 1

Hairy Baby
@HairyBabyTees



Follow

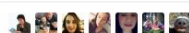
Verified By Visa...eeeeeeeeaaaaaghghhhhhhh!!!!
#deepbreaths #staycalm

RETWEET

1

LIKES

9



10:46 AM - 6 Sep 2016

Retweet 1

alister mcnaught
@alistaarm

Follow

Verified by Visa - the consumer's best friend. How often I hit that barrier and think to myself "I have no idea what my password is and I could actually live without this purchase". V by V has saved me hundreds of pounds on impulse purchases. Thankyou!!

12:03 AM - 20 Apr 2019

1 Retweet 4 Likes



Reid Conti
@reidconti



Follow

Has @VerifiedByVisa or @mastercard #securecode ever fucking worked for anybody, in the history of the world? Fuck your shitty broken schemes

7:06 PM - 16 Sep 2016

Anna Freeman
@JuneDown



Follow

Im Bestellvorgang natürlich den Mastercard SecureCode vergessen, welcher nun gesperrt ist



View translation

8:29 PM - 15 Sep 2016

Retweet 1



3D Secure Research

3DS takes an average of **37 seconds** to complete

Conversion by Issuer ranges from **68 to 92%**

9% "frictionless" (less than 5 seconds)

"Improved 3DS" loses 19% of payments



Status Quo

3D Secure is bad for business

Merchants can decide when & if to Authenticate

Authenticate high risk transactions only

#ravcon19



PSD2 changes everything

#ravcon19



PSD2

| Merchants can decide if and when to Authenticate



PSD2

~~Merchants can decide if and when to Authenticate~~

Merchants can only turn off Authentication...



PSD2

~~Merchants can decide if and when to Authenticate~~

Merchants can only turn off Authentication...
if they're very good at fraud detection...



PSD2

~~Merchants can decide if and when to Authenticate~~

Merchants can only turn off Authentication...
if they're very good at fraud detection...
and **if** the Issuer agrees.

#ravcon19



Strong Customer Authentication

| SCA = 3D Secure for Card Payments



Exemptions from SCA

Low **Value** Transactions

Low **Risk** Transactions

Recurring Transactions (of the same value)



Low Value exemptions

Under €30

Low Value can still be High Risk

Issuer keeps count of number and value of Low Value Exempt transactions

Black box - merchants have no idea if it's transaction #1 or #6



Low Risk Exemptions

Transaction Risk Analysis (TRA) is hard
TRA is now Regulated



Low Risk Exemptions

Payment service providers shall ensure that the transaction monitoring mechanisms takes into account, at a minimum, and on a real-time basis, each of the following risk-based factors:

- **lists** of compromised or stolen authentication elements;
- **the amount of each payment transaction;**
- **known fraud scenarios** in the provision of payment services;
- **signs of malware infection** in any sessions of the authentication procedure.
- **the previous spending patterns** of the individual payment service user;
- **the payment transaction history** of each of the payment service provider's payment service user;
- **the location of the payer and of the payee** at the time of the payment transaction providing the access device or the software is provided by the payment service provider;
- **the abnormal behavioural payment patterns** of the payment service user in relation to the payment transaction history;
- in case the access device or the software is provided by the payment service provider, a **log of the use of the access device** or the software provided to the payment service user and the abnormal use of the access device or the software.

irrespective of the specific arrangements of the transaction monitoring mechanisms, an electronic payment transaction is identified as posing a low level of risk only where the following conditions, in combination with the risk analysis referred to in point b) of this paragraph, are met:

- I. **no abnormal spending or behavioural pattern** of the payer has been identified;
- II. **no unusual information about the payer's device/software access** has been identified;
- III. **no malware infection** in any session of the authentication procedure has been identified;
- IV. **no known fraud scenario** in the provision of payment services has been identified;
- V. **the location of the payer** is not abnormal;
- VI. **the location of the payee** is not identified as high risk.

#ravcon19

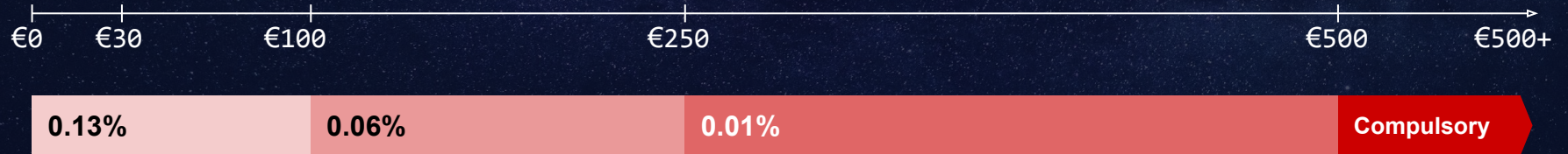


Low Risk Exemptions

| Is your Rules Engine compliant?

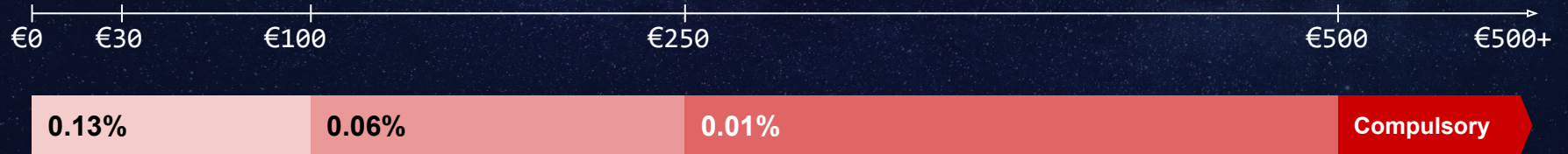


Fraud rates really matter





Is your Acquirer good enough?





3D Secure

Version 1 failed. Version 2 is.... better

Better User Interface & more data for Issuers

3DS2 is the Least Worst Option



3D Secure 2

Better user interface for card holders to authenticate

Issuers can do their own risk analysis and authenticate "Frictionlessly"

"Improved 3DS" loses 19% of payments



Maximising Acceptance in a PSD2 World

- Much more complex than today
- Each Issuer will be different
- 3D Secure v1 and v2 will coexist
- Conversion will be a big differentiator



Advice to merchants

- Use an Acquirer with low fraud rates
- Outsource your TRA for the best acceptance rates
- Maximise SCA exemptions to keep conversion high
- Use 3DS2 for the least worse consumer experience



Advice to merchants

- Use an Acquirer with low fraud rates
- Outsource your TRA for the best acceptance rates
- Maximise SCA exemptions to keep conversion high
- Use 3DS2 for the least worst consumer experience

Use Ravelin Accept to manage all of this for you!

Fin.



Ravelin's Secure Growth Summit 2019



Technology and the analyst

ravelin.com



Our Panel

JUST EAT

Lora Walsh
Global Fraud Manager

JAGEX

Dave Parrott
Payments Services Director

**green man
gaming**

Daniele Thillman
SVP Head of Risk and DPO



Closing Remarks