Remote IDV & Due Diligence:

Embracing Technology as a Tool to Optimise KYC/AML Compliance Procedures whilst Minimising Costs.

iSignthis Ltd (ASX:ISX / FRA : TA8)

(SWIFT BIC : ISEMCY21)

N J (John) Karantzis

B.E. LL.M M.Ent FIEAust CPEng EurIng Adj

Managing Director & Group CEO

iSignthis®

MLROs.com

Contents

- The introduction of the PSD2 & 4th AML Directive / 2017 MLR's
- (Enhanced) Customer Due Diligence (remote operations)
- Solving the KYC compliance via RegTech

1. What do we do?

iSignthis automates AML/CTF KYC and transaction processing

iSignthis Ltd is an EEA authorised EMI/MFI which automates AML/CTF Enhanced Due Diligence KYC & transaction monitoring via its payments and identity processing platform (Paydentity™) for AML regulated sector businesses including:

- Financial Institutions,
- banks, lending, crowdfunding, pension funds,
- securities / equities,
- FX, CFD, binaries, and futures traders,
- gaming, wagering, betting, casino's,
- money services businesses,
- payment service providers,
- insurance providers,
- real estate,
- digital currency platforms,
- eWallets, Fintech,
- other AML/Patriot Obligated businesses, and
- ***Ourselves, as an EU regulated Monetary Financial Institution!***

GDPR READY

PCI DSS COMPLIANT

bsi. ISO/IEC 27001 Information Security Management

ico. Information Commissioner's Office
REGISTERED WITH THE UK ICO # ZA217768

AUTHORISED BY THE CBC # 115.1.3.17 ISIGNTHIS EMONEY LTD

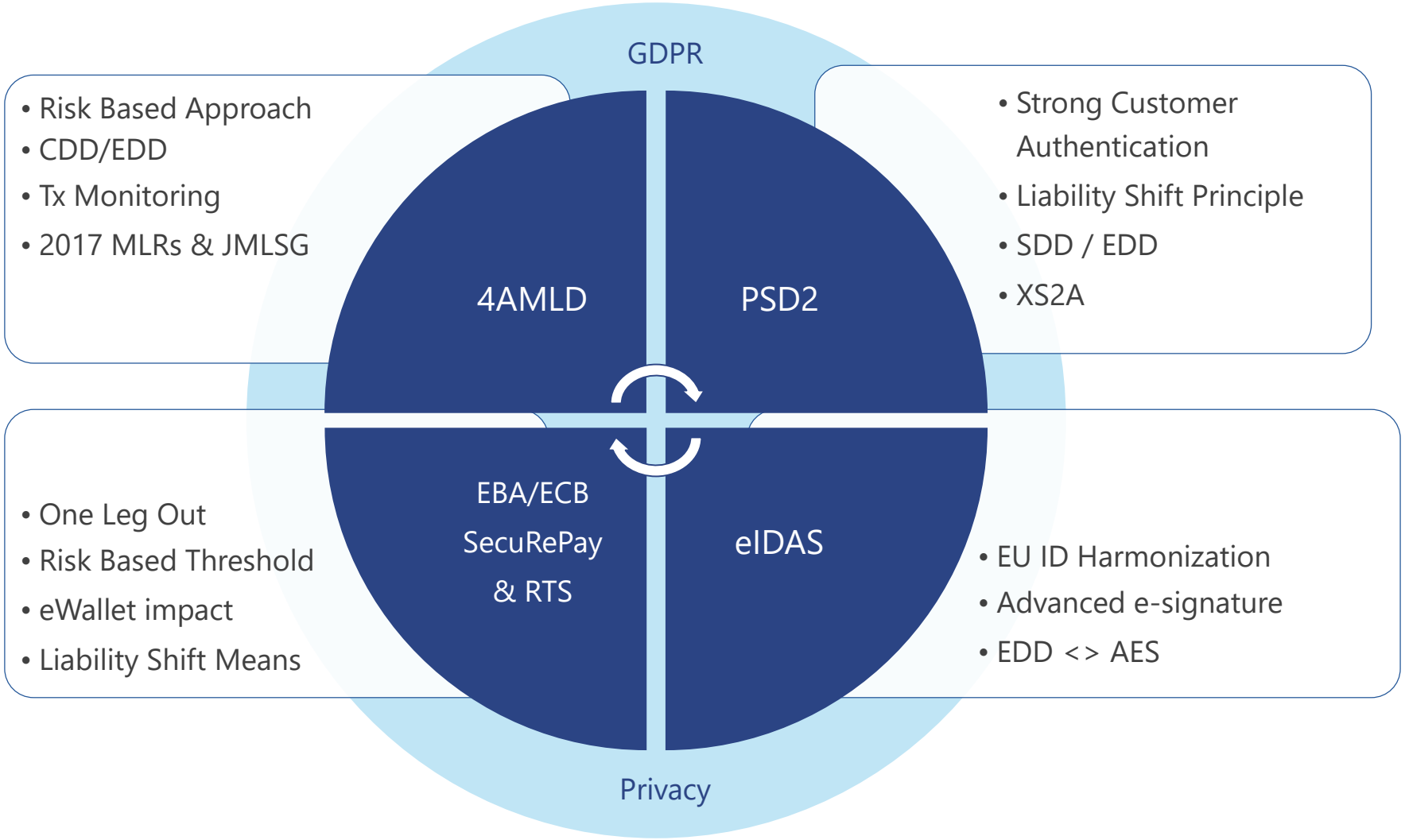
STOCK CODE : ISX

BÖRSE FRANKFURT
STOCK CODE: TA8

JCB MasterCard
Principal Member

ECSG european cards stakeholders group
Foundation Member
Board Member

2. The EU Identity and Payment Landscape



3. PSD2 : Regulatory evolution is driving change

4AMLD and PSD2 require a more rigorous approach to IDV & Authentication

PSD2 & transactional payment processing authentication

- PSD2 is technological and business case neutral – this is a central tenet of the directive.
- All online payments > €30 required to undergo Strong Customer Authentication (SCA) using a method of Two Factor Authentication (2FA) to be linked to the card's owner. (EBA RTS, e-verification, ECB KC6.1)
- SCA does not necessarily mean 3DSecure! Other options available. PSD2 Liability Shift is via ECB Governance framework of card schemes (See SecurityofIPayments, KC7.6 & ECB Card Governance Framework)
- SCA not required for MOTO (See EBA RTS Comments [73])
- The use of 2FA without proving a persons identity first, is known as Strong Authentication (SA) – this is commonly used by some tech companies and is not compliant under the current PSD2 regulations. (See PSD2 Article 4, (29) & (30), EBA RTS Comments [1] and [274])

4. PSD2: Regulatory evolution is driving change

4AMLD and PSD2 are requiring a more rigorous approach

PSD2 & transactional payment processing authentication

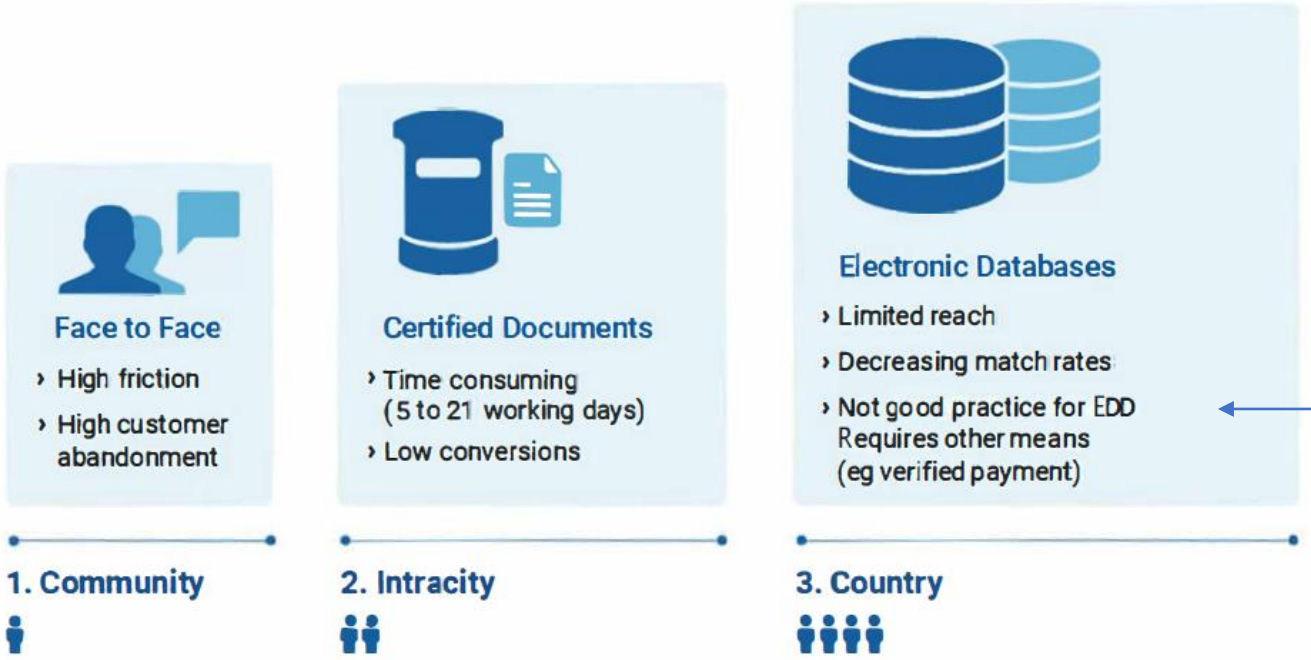
- The risk based approach allowed for by the EBA in its RTS at Article 16 are set between 0.13% fraud on € 100 average to 0.01% to €500 average, with € 500 being the cap after which SCA must apply.

- The risk based approach allowed for by the EBA in its RTS is farcical, and was a late addition to the RTS based upon industry lobbying. The fraud rates specified are required to be so low, that PSP's will simply apply SCA rather than risk liability. (See ECB 4th Card Fraud report – .57% / 0.45% is more likely when 3DS not applied)

- One leg out transactions will present a massive challenge for Payment Service Providers (PSPs) to overcome. Verifying transactions of cards issued outside the EEA, when 3DSecure is not available will cause massive abandonment, as PSP unlikely to accept liability (RTS Rationale [16] and Comments [295], FCA Daft PSR Guidance)

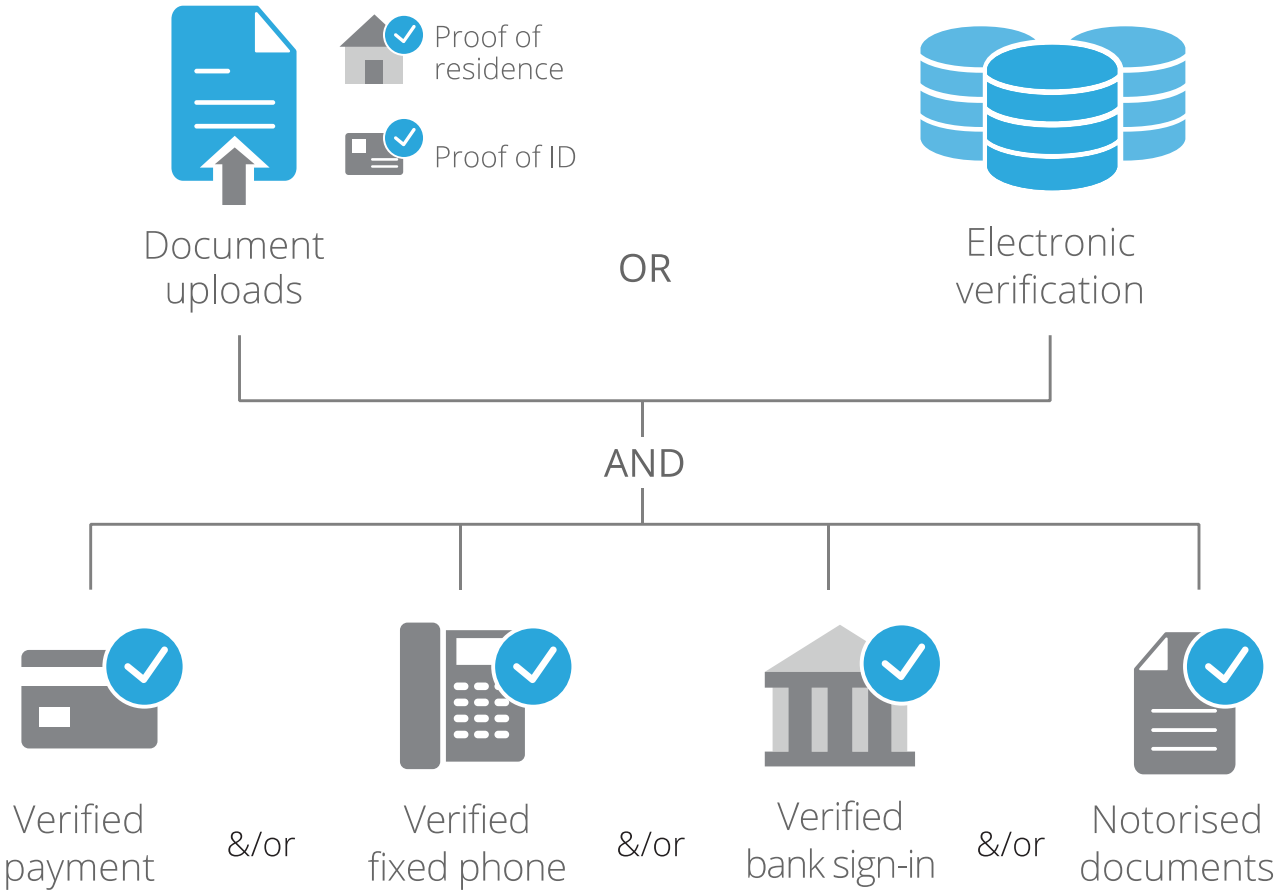
5. 4AMLD / 2017 MLR's : Establishing Identity

Three main accepted means to perform **enhanced due diligence** Know Your Customer (KYC), all of which **rely on banking or government (original) sources.**



2014 JMLSG at 5.3.71 or 2017 JMLSG at 5.3.89/90.

6. Cysec, Austrac & UK JMLSG Requirements



Satisfying Regulations:

Either Doc Uploads or Electronic Verification AND one of the second line.

By verifying payment, we confirm:

a) Source of funds
b) that funding is available
c) Instantly for cards or within 2 business days for SWIFT/SEPA : completing enhanced CDD of customer whilst onboarding customer and taking payment!
d) Paydentity™ incorporates bank issued credit and debit cards, as they are not only the leading online payment source, but also the largest single source of KYC data accessible globally.

7. 2017 Revised JMLSG – Remote Customer

- 5.3.90 The additional verification check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:

- **requiring the first payment to be carried** out through an account in the customer's name with a UK or EU regulated credit institution, or an assessed low risk jurisdiction;

- verifying additional aspects of the customer's identity (see paragraph 5.3.29);

- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;

- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, is required to be returned completed or acknowledged without alteration);

- requiring copy **documents to be certified by an appropriate person.**

7. 2017 Revised JMLSG – Remote Customer

5.3.89 Where identity is verified electronically, [or] copy documents are used, or the customer is not physically present, a firm should apply an additional verification check to manage the risk of impersonation fraud. In this regard, firms should consider:

verifying with the customer additional aspects of his identity (or biometric data) which are held electronically; or

requesting the applicant to **confirm a secret code or PIN**, or biometric factor, that links him/her incontrovertibly to the claimed electronic/digital identity – such codes, **PINs or other secret data** may be set up within the electronic/digital identity, or may be supplied to a **verified mobile phone**, or through a **verified bank account**, on a one-time basis, or

following the guidance in paragraph 5.3.90.

8. ‘Recency’ of data

What does “recency” mean? In practice? From a regulatory perspective?

CySec, June 2016, Appendix IV, paragraph c:
Electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information and negative information.
and
electronic databases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alter.

Austrac Regulations :
Rule 4.10.2 (c) “how the data is kept up-to-date; ”

2017 Revised UK JMLSG :
5.3.51 “for example, in relation to data sources used, or recency of information”
5.3.52 “The information maintained should be kept up to date, and the organisation’s verification – or re-verification - of different aspects of it should not be older than an agreed set period.”

9. Lets look at Electronic Verification – UK+AUS style – Historic Credit Reference File

JOAN LOUISE SMITH
REFERENCE: PAS 1234567

veda applied intelligence

Personal Information

Identity Details	
Name:	Joan Louise Smith
AKA (Also Known As)	Joan Louise Harrison
Date of Birth:	15 Jan 1975
Gender:	Female
Driver's Licence Number:	12364578
Address History:	15 Tree Avenue RANDWICK NSW 2031 1/63 View Street CURL CURL NSW 2096 29/90 Fuller Street KENSINGTON NSW 2033 10 Beach Street MOOLOOLABA QLD 4557
Employment History:	EASTFIELD PRIMARY SCHOOL THE DEPARTMENT STORE

Financial Account – Express Bank

Consumer Credit Liability Information	
Name of Provider	EXPRESS BANK
Account Type	Credit Card
Account Number	EPB0075
Account Open Date	11 Apr 2013
Loan Payment Method	
Term Type	Revolving
Term of Loan	Unspecified
Relationship	Principal's Account (sole or joint borrower)
Secured or Unsecured	Unsecured
Balance Limit	$10,000
Closed Date	

9. DNA of a 'Real time' Electronic Payment Message

Card DNA

DEVICE DATA
(Finger Print, IMSI,
CPE, Language, OS)

EXTERNAL REFERENCES
(Government database,
Credit reference)

AUTHENTICATION + VALIDATION
(Geodata, Device Data, SAD,
Phone Number, SMS, HLR Records)

DELIVERY DATA
(Address, Phone, Email,
IM, Social Media)

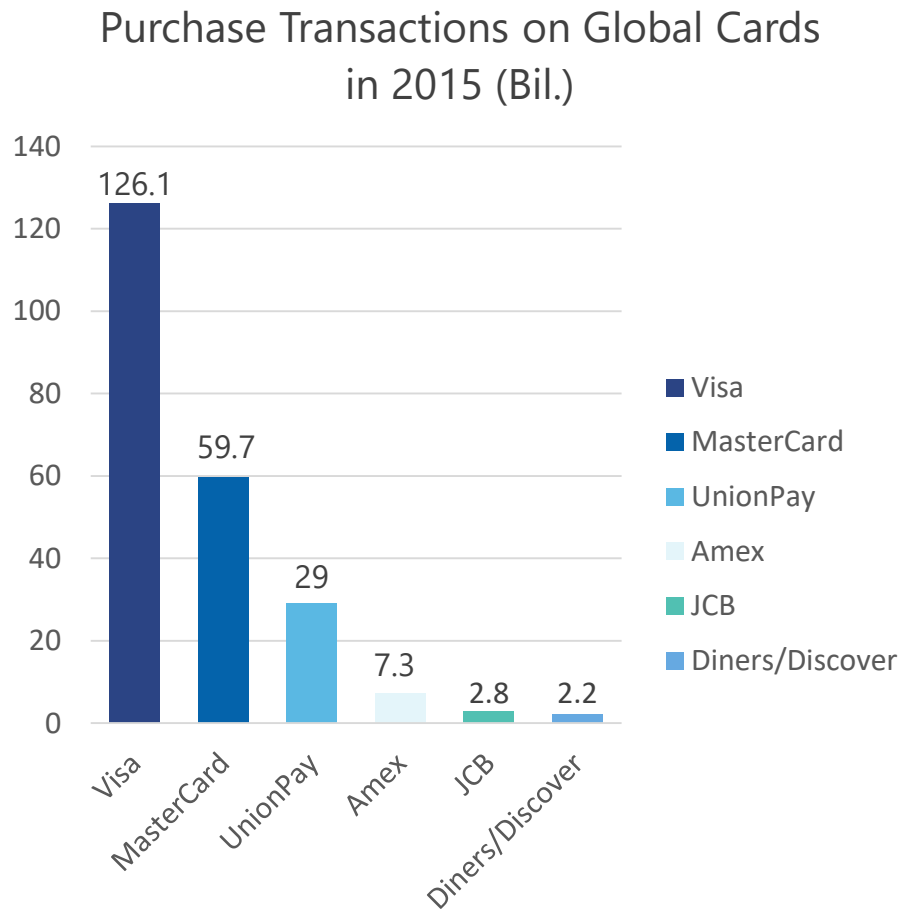
PAYMENT DATA
(Merchant, Acquirer, Card Details,
Name, Amount, Place, IIN Data + Coun-
try of Issuer, Transaction History)

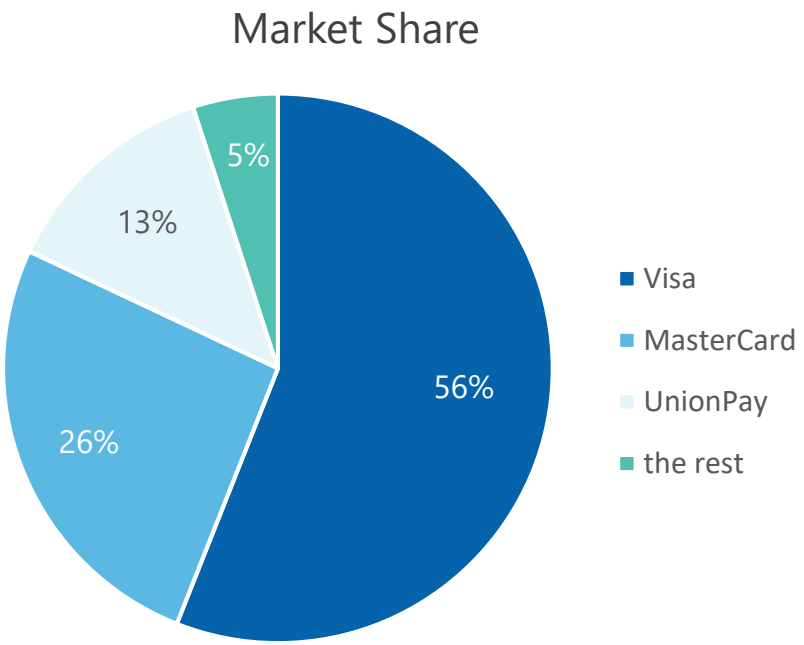
NETWORK DATA
(IP Address, Carrier, Channel,
Route, HLR Location)

Swift / SEPA DNA : Originating Bank, Name, Amount, Currency

Shared with CRA File

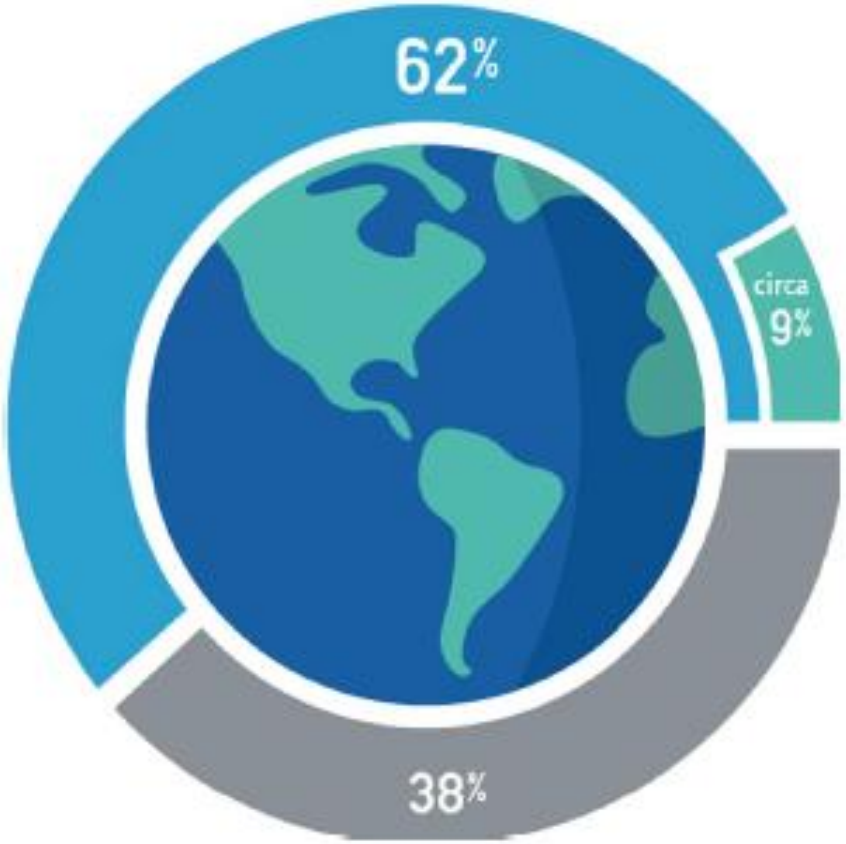
10. Cards – The Largest Payment & KYC Source





- 9.5Bn cards on issue, globally
- According to Nilson, 3.5Bn are unique
- McKinsey estimates that 51% of the world's population is "banked" – corresponding also to ~3.5Bn persons.

11. World Population – 62% Banked / 38% Unbanked, with CRA Data accessible for ~ 9%



62% Financially Included (banked)

62% of the world's population are banked, making 'bank verified' persons the largest electronically accessible 'reliable and independent' source of KYC data.

circa 9% Data Brokers Circa

Data brokers can only identify Circa 9% of the world's population, providing merchants with a limited reach and low conversion rates.

38% Unbanked

38% of the world's population don't have a bank account and are unable to pay for services via a electronic payment, credit or debit card.

Source: Worldbank 2015 Findex, http://datatopics.worldbank.org/financialinclusion

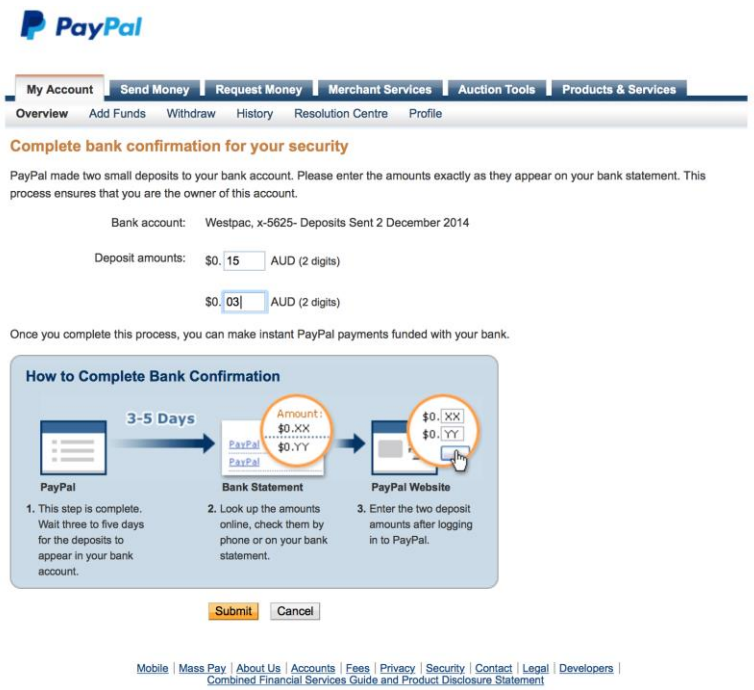
12. Verifying a Customer through Creating a 'Secret'

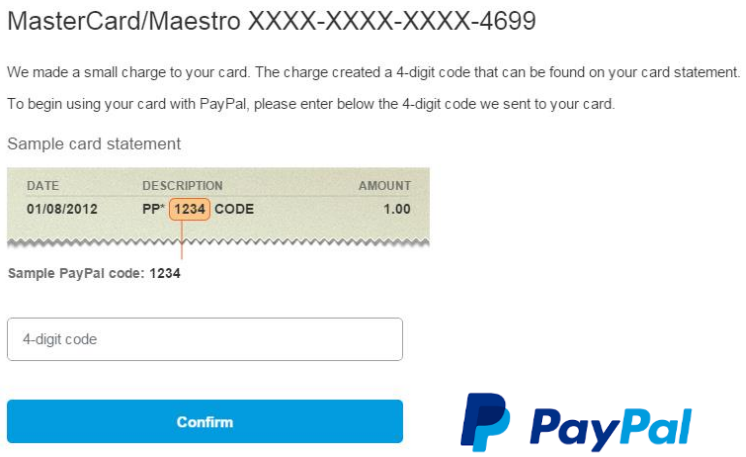
5.3.89 Where identity is verified electronically, [or] copy documents are used, or the customer is not physically present…….
requesting the applicant to confirm a secret code or PIN, or biometric factor, that links him/her incontrovertibly to the claimed electronic/digital identity – such codes, PINs or other **secret data** may be set up within the electronic/digital identity, or may be **supplied to a verified mobile phone, or through a verified bank account,** on a one-time basis, or following the guidance in paragraph 5.3.90.

Commentary
What's a 'verified' mobile phone?
The UK has no register of owners of mobiles,
purchasing prepaid does not require ID,
sending a SMS proves – what?
Even countries like Germany that require ID to purchase have difficult access to register of ownership
China has a register of owners of phone …but you'd expect that.

Bank and Credit Cards – several methods (many patented) exist to verify – beware of their use!
Eg Paypal https://www.epo.org/law-practice/case-law-appeals/recent/t090844eu1.html

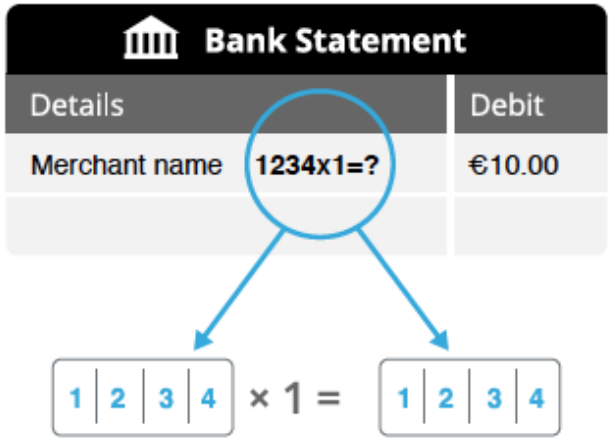
12. Examples of Creating Dynamic Secrets to satisfy Key parts of 2017 JMLSG & PSD2 SCA Registration



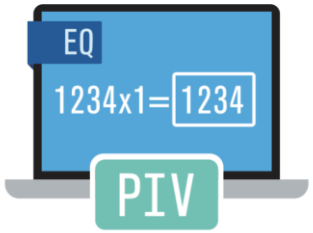


PayPal

Example:



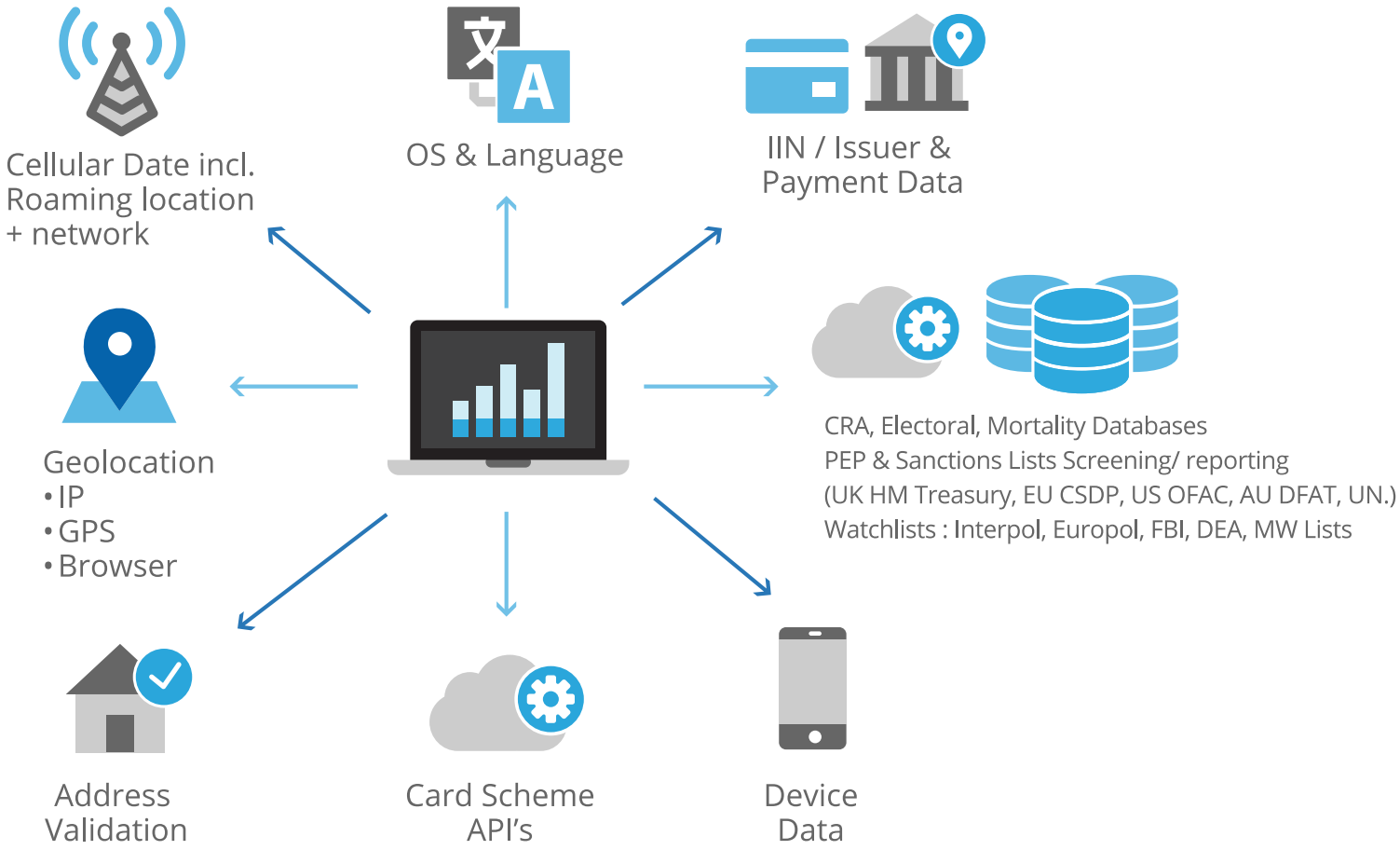
PIV



Caution, Patents Applicable : iSignthis patents apply to creating a secret via Equation, Anagram, Word to Match to Picture or divide payments
US6032863 , US8131617, US7588181, US8805738, US7765153
US8620810, CA2791752A1, CN102812480A, EP2553642A1, US20120323791, US20140222677, AU2012261779, AU2011235612 , AU2010100533, ZA2012/06455, SG201206344-2, WO2011120098A1

NB : Paypal Inc holds European and US patents on random “micro deposits” to an account and random secret inserted into descriptor.

13. Real Time Analytics – Screening and Reporting



14. Questions you should be considering

For your PSP under the PSD2:

- Will your PSP impose 3D Secure on all transactions?
- How will your PSP satisfy the 'one leg out' requirements, so you can accept cards from outside the EEA?

For your KYC Electronic Verification Provider

- How is 2+2 achieved outside the UK and Australia?
- What dynamic/real time element is used to satisfy 'recency' / 'up to date' requirements?
- What are your 'reliable and independent' data sources outside UK and Australia?
- Who are these sources shared with and are they registered with ICO equivalent?
- How often are they updated, and how are you alerted if they are / are not?

Where document uploading is used

- Uploaded Copy documents are not sufficient by themselves to satisfy UK, Australia, Cyprus, US or any EU regulatory regime for CDD – how do you verify to an enhanced due diligence standard per 4AMLD/JMLSG/CySec etc?

Questions?

- iSignthis Ltd (ASX:ISX / FRA : TA8)
- SWIFT/BIC : ISMCY21
- Contact @ iSignthis.com