Analytics in Action

SAS Analytics Insights Roadshow

7 June 2019 | Bangkok

Leveraging AI To Combat the Latest Challenges with Fraud in the FSI Sector

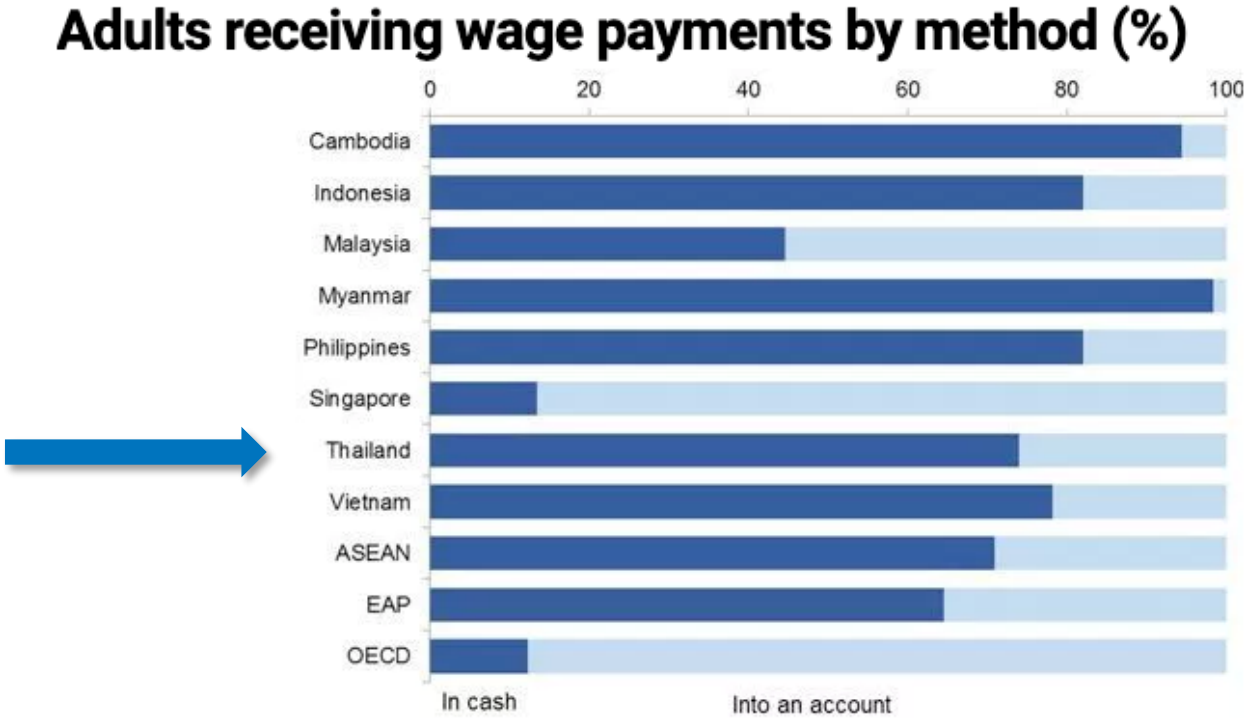
The Opportunities & Challenges

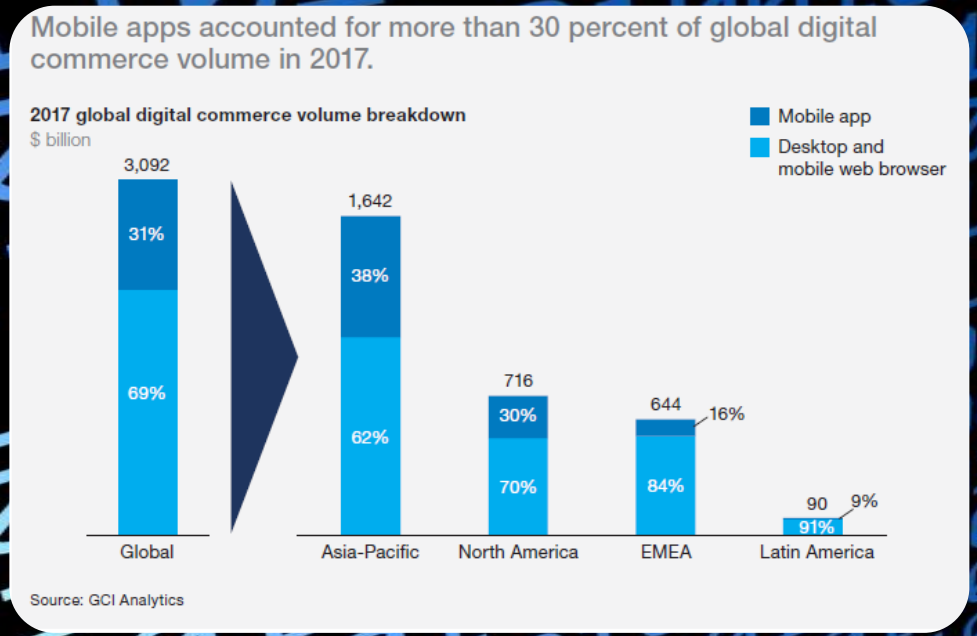
The Opportunity

Thailand Business News

Published 3 years agoon February 13, 2016
By **Boris Sullivan**

In ASEAN countries, only 29% of workers reported receiving their monthly salaries through an account from a financial institution, while the remaining 71% is paid in cash by their employers. In Thailand, about 70% of workers are still paid in cash.





Data Size , Variety & Compute Power

1950s

1980s

Past to Present

2010's

Present

https://www.mckinsey.com/.....Global-payments-map-2018.ashx

Faster Payments Will Bring More Opportunities

* in development
\# consideration

The Opportunity

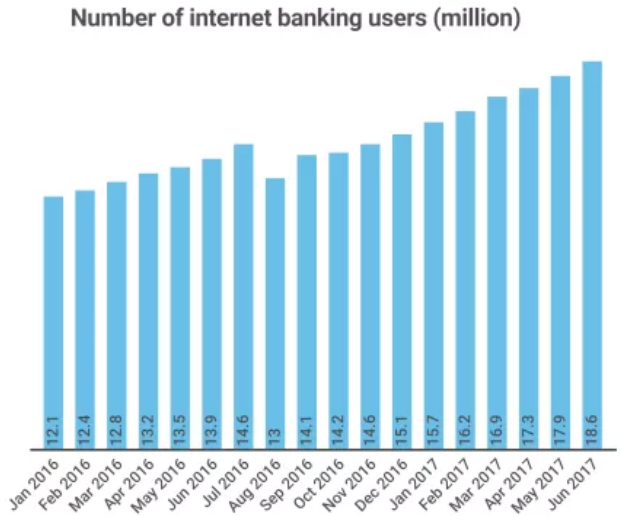
ASEAN Today

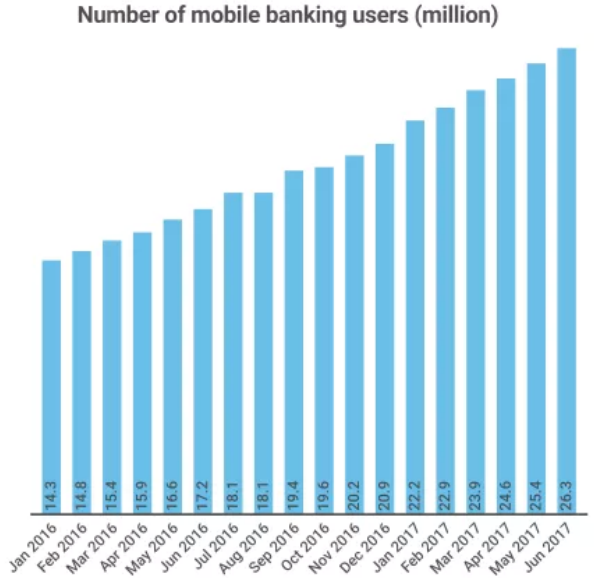
FEBRUARY 2, 2018

By Oliver Ward

Thailand could go cashless within three years

Digital payments took off in Thailand in 2017. The volume of mobile payments for June 2017 reached **694 billion baht** (US$22.1 billion). It is a significant increase from **440 billion** (US$14 billion) the previous June. Mobile and internet banking has been steadily increasing. The conditions are ideal for the expansion of the e-payment industry.





sas

The Opportunity

ASEAN Today FEBRUARY 2, 2018 By Oliver Ward

Thailand could go cashless within three years

On average, small businesses increase sales **by 17%** by installing an e-payment option. For large businesses, this figure rises to **22%**. This occurs for two reasons. Firstly, it reduces sales lost from customers who do not have enough cash on their person. Secondly, e-payment data provides information on consumer spending habits. Businesses can analyse this data and streamline promotions accordingly.

Is Thailand ready to go cashless?

The chairman of the Thailand E-Payment Trade Association (TEPA) believes Thailand could go cashless within three years. Punnamas Vichitkulwongsa **made the comments** in August 2017.

There are still barriers to overcome

Mr Nuttawit Polwattanasuk is the Managing Director of the e-commerce company, LnwShop. He believes security is a major concern for shoppers. It is one of the biggest problems facing the e-payment industry. "Many Thai shoppers still voice their concerns about the safety of online payments," he **said**. Rolling cashless payment technologies out to rural areas is another problem.

Real Time = Right Time

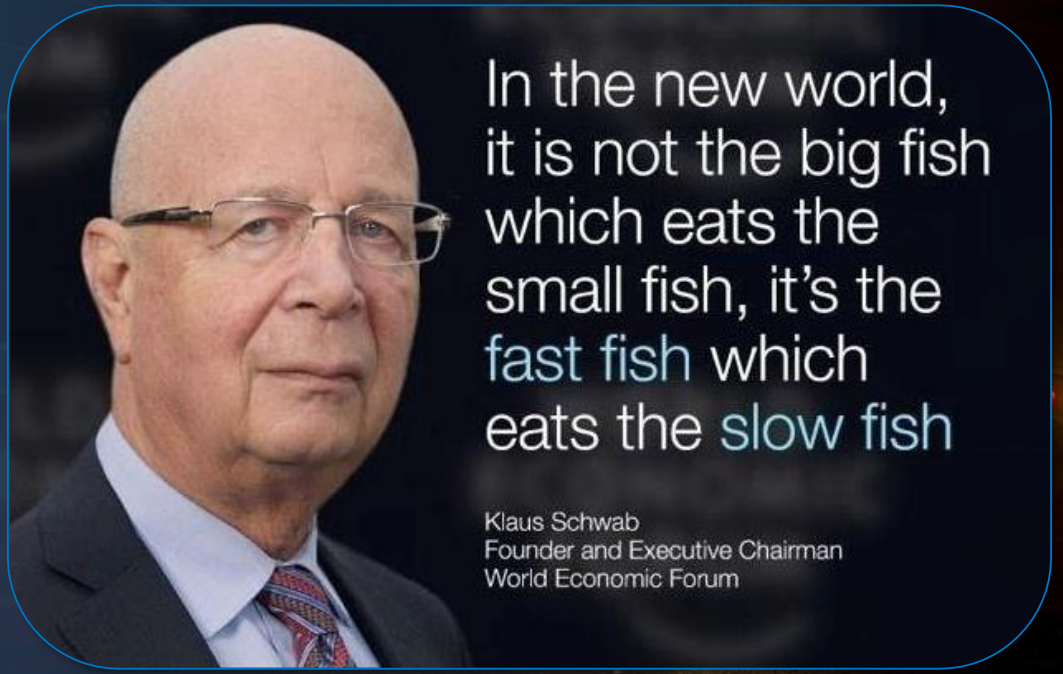
Omni-Channel

Money in Moments

Customers only want to see convenience

Criminals want to see opportunities and points of compromise

The Speed of Light



The Speed of Right

sas

Online - It Is A Fine Balance

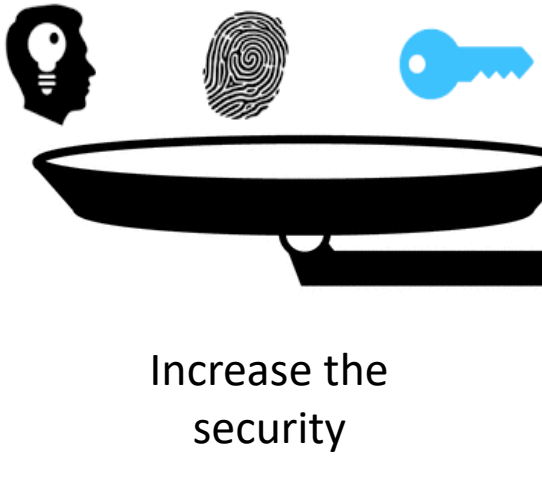
Customer Frustration

Criminal Opportunity

Something you know

Something you are

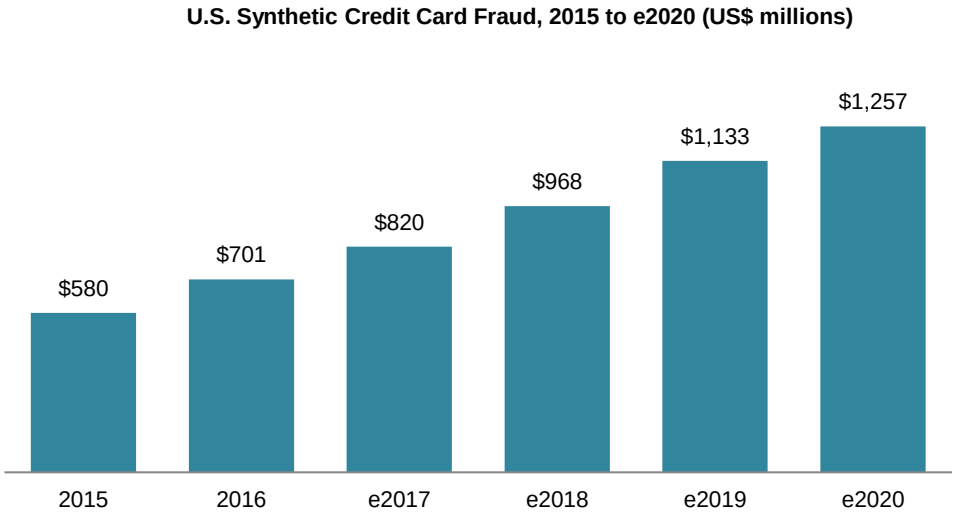
Something you have



Increase the security

Reduce customer friction

Synthetic Identity

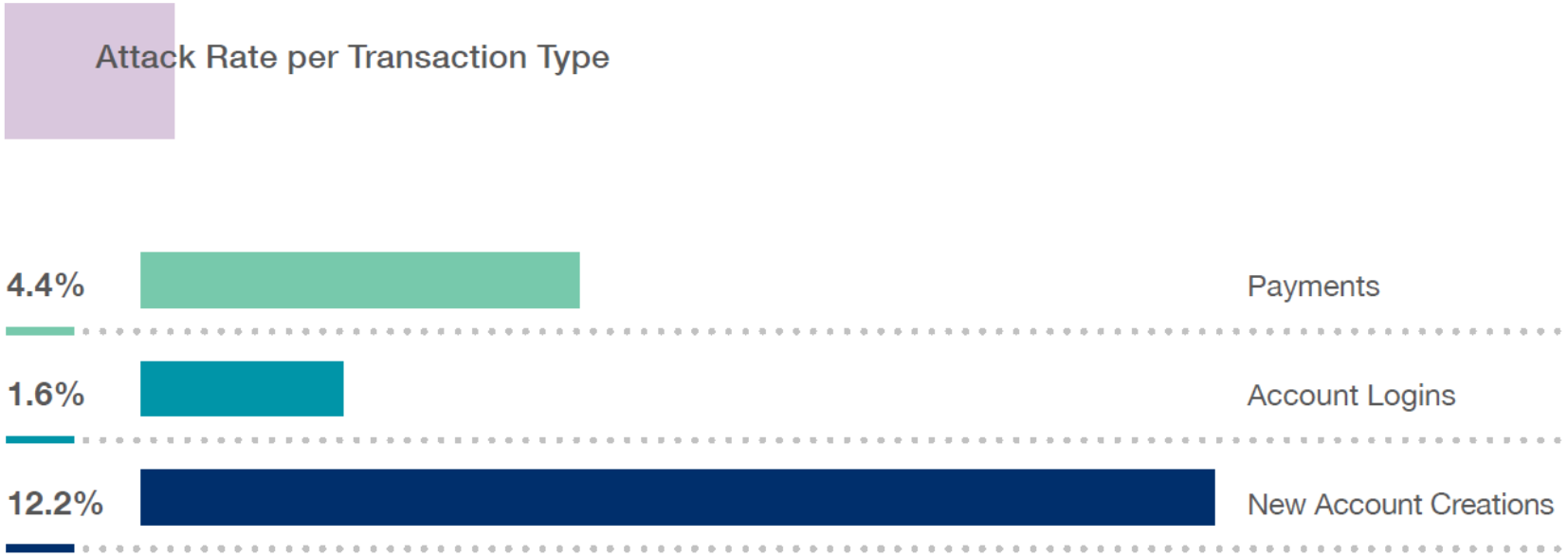


Source: Aite Group, 2017

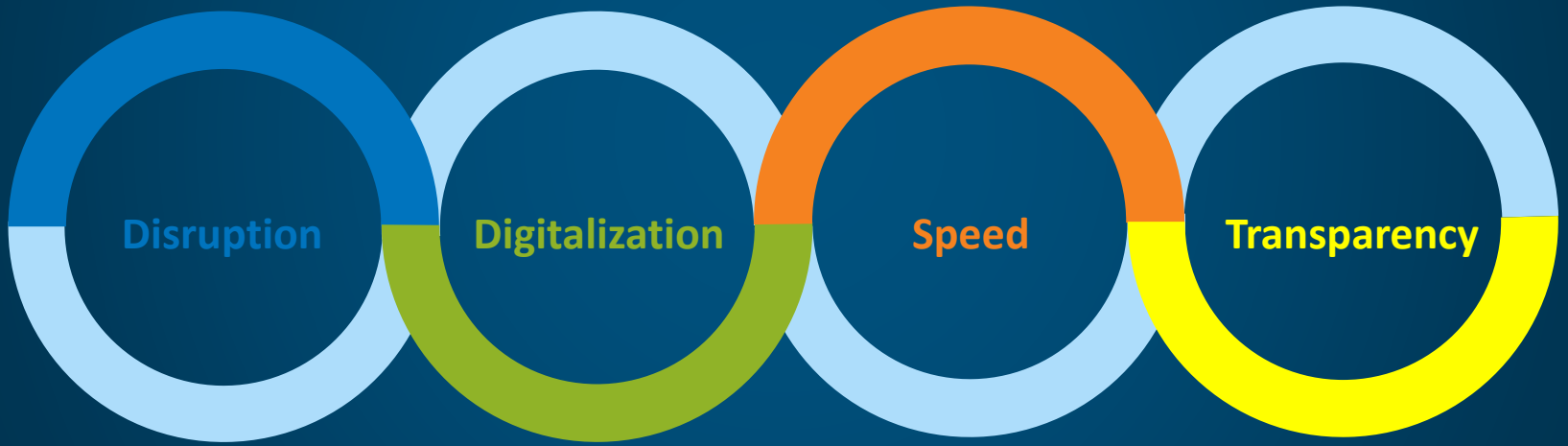
Not just a fraud and credit risk problem—AML concerns as well

Identities nurtured 6 months to 5 years, average loss per account $10K+

Where Are The Risks?



Global pressures created by…



IN YOUR LANGUAGE..

Rising false positives, increasing channels, volumes & risk

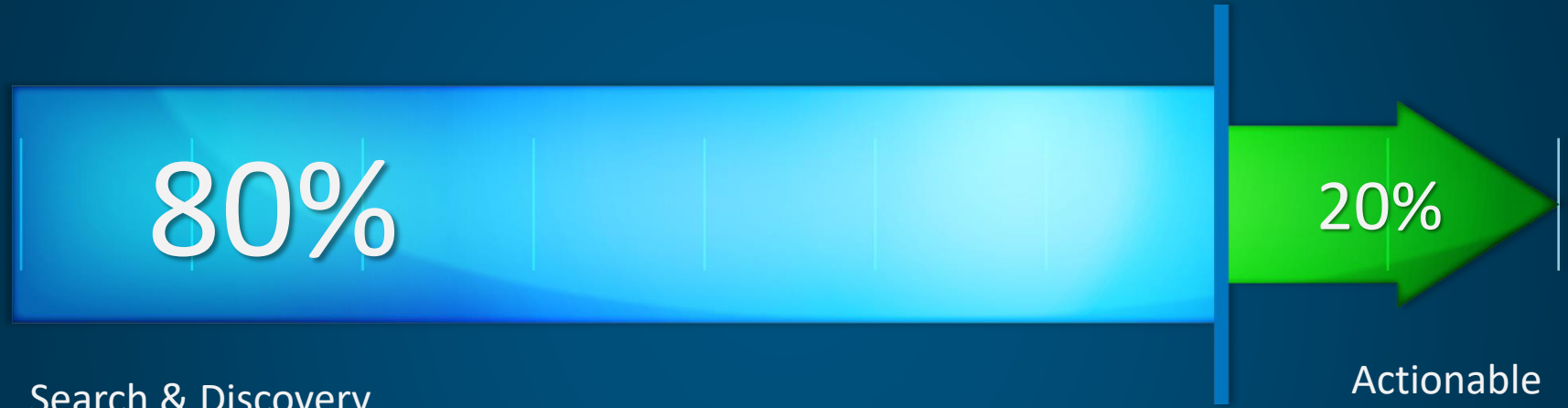
“Faster payments” moves settlements to real-time

Automation of manual processes aka “Robotic Process Automation”

Regulatory scrutiny and transparency – know your customer and your risk

Pressure to use Artificial Intelligence & Machine Learning

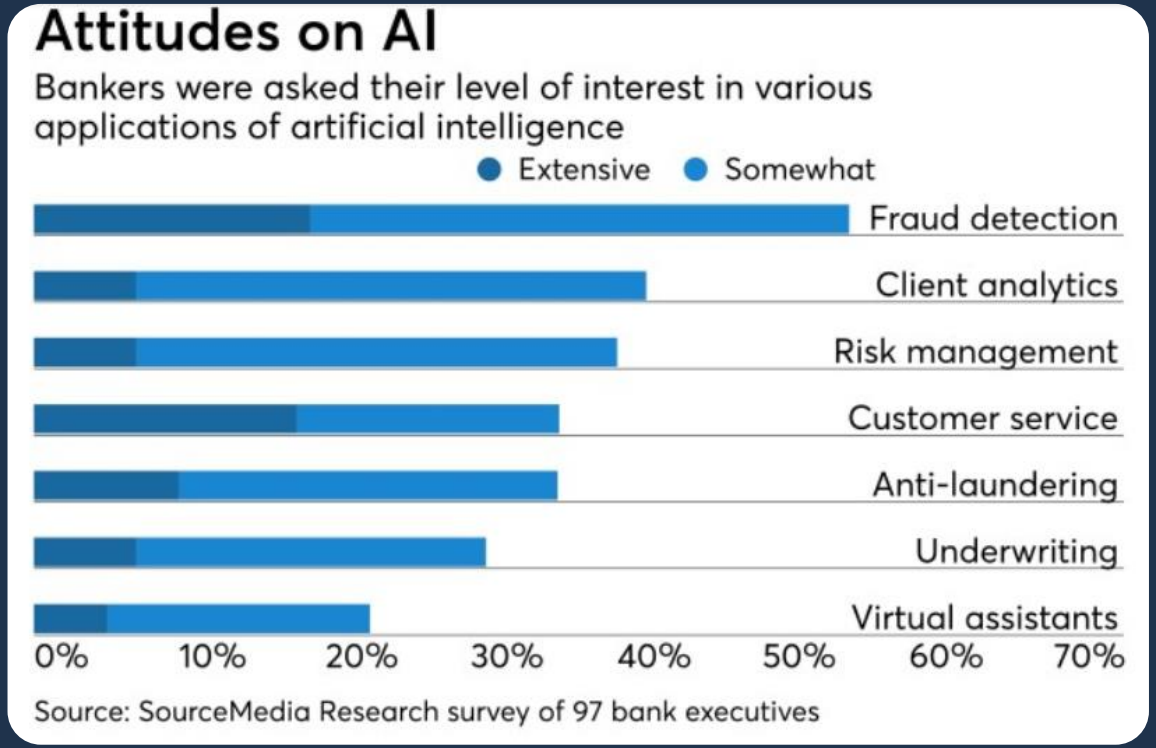
The Real Challenge



Search & Discovery
Labour intensive: Identifying relevant information, searching various data sources, “formatting” data for a specific tool, processing, applying “analytical techniques” within a tool, typically ad-hoc and manual.
OFTEN TOO LATE TO PREVENT IT

Actionable Analysis
Applying specific tradecraft, vetting of information

So Where Does Analytics Fit In?

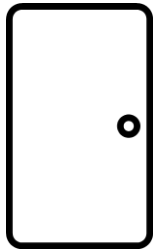


Barriers aside, if you could design from scratch a new enterprise fraud prevention platform, what elements would it include? (select three that apply)

Information Security Media Group, Survey - 2018

Focus of fraud detection

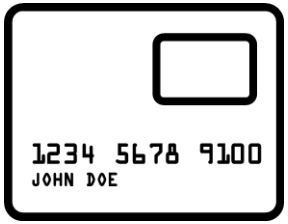
"move left"!



Identity validation

Authentication & user behaviour

Customer & event profiling

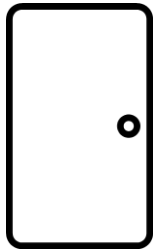


Transaction/Payment Monitoring

Debt Collection

Fraud Management Analytics – Early Days

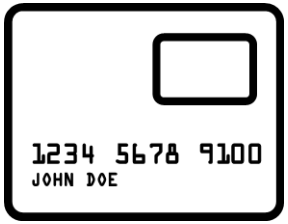
Focus Areas



Identity validation

Authentication & user behaviour

Customer & event profiling

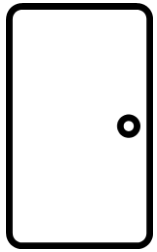


Transaction/Payment Monitoring

Debt Collection

Fraud Management Analytics – Last 10 Years

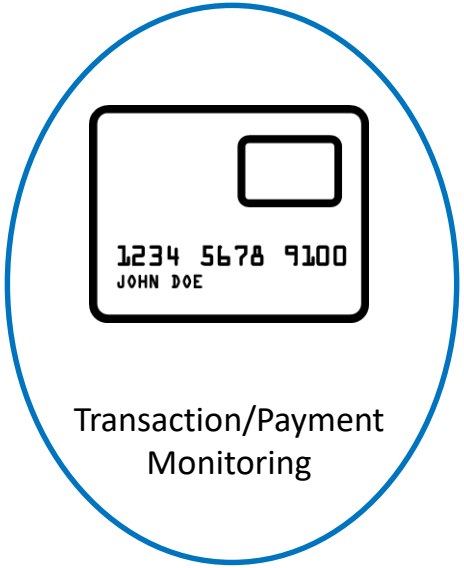
Focus Areas



Identity validation

Authentication & user behaviour

Customer & event profiling

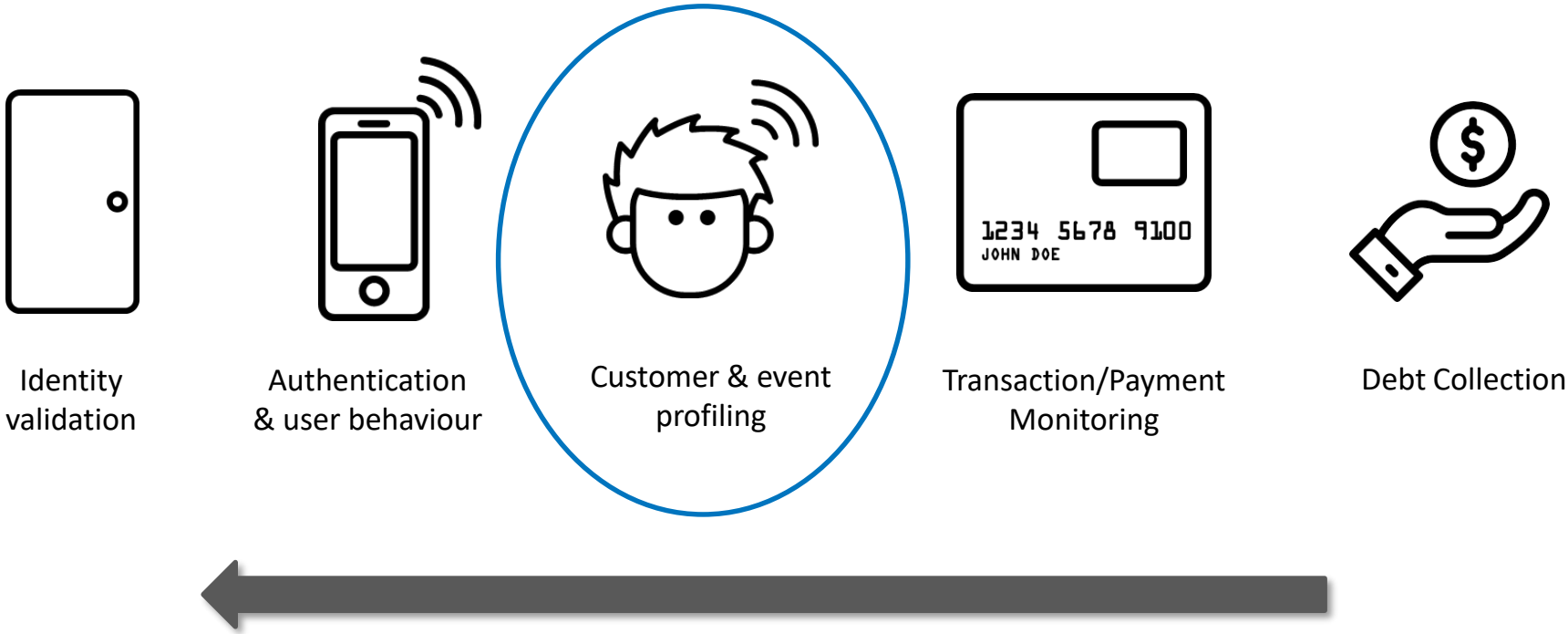


Transaction/Payment Monitoring

Debt Collection

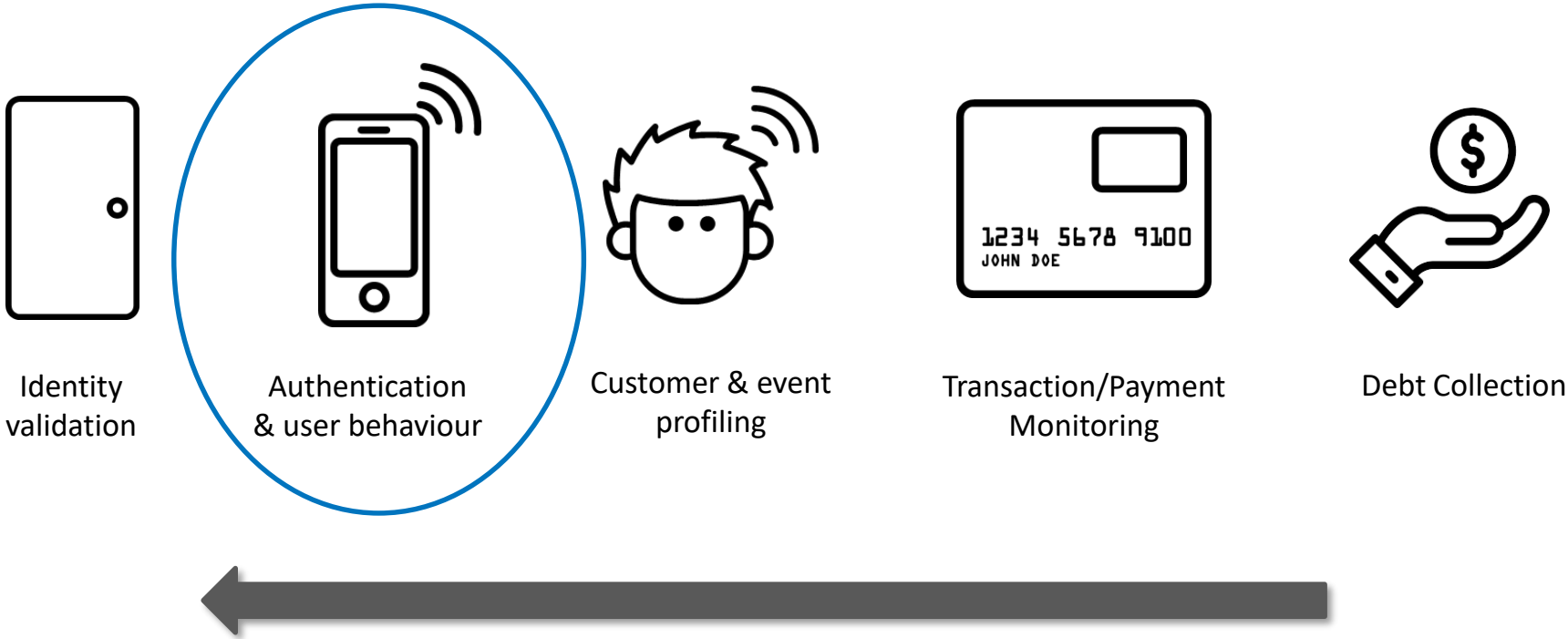
Fraud Management Analytics – Last 3 Years

Focus Areas



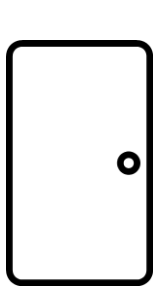
Fraud Management Analytics – Present & Future

Focus Areas



Fraud Management Analytics – Present & Future

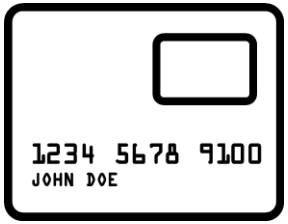
Focus Areas



Identity validation

Authentication & user behaviour

Customer & event profiling

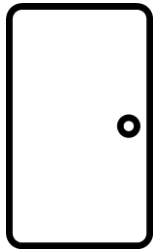


Transaction/Payment Monitoring

Debt Collection

Fraud Management Analytics – Present & Future

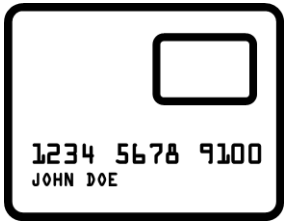
Leveraging AI – Focus on them all!



Identity validation

Authentication & user behaviour

Customer & event profiling

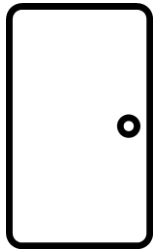


Transaction/Payment Monitoring

Debt Collection

Fraud Management Analytics – Present & Future

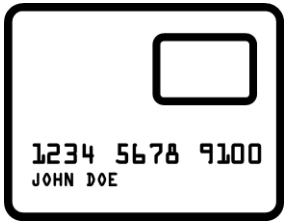
To give a true Customer-Centric view



Identity validation

Authentication & user behaviour

Customer & event profiling



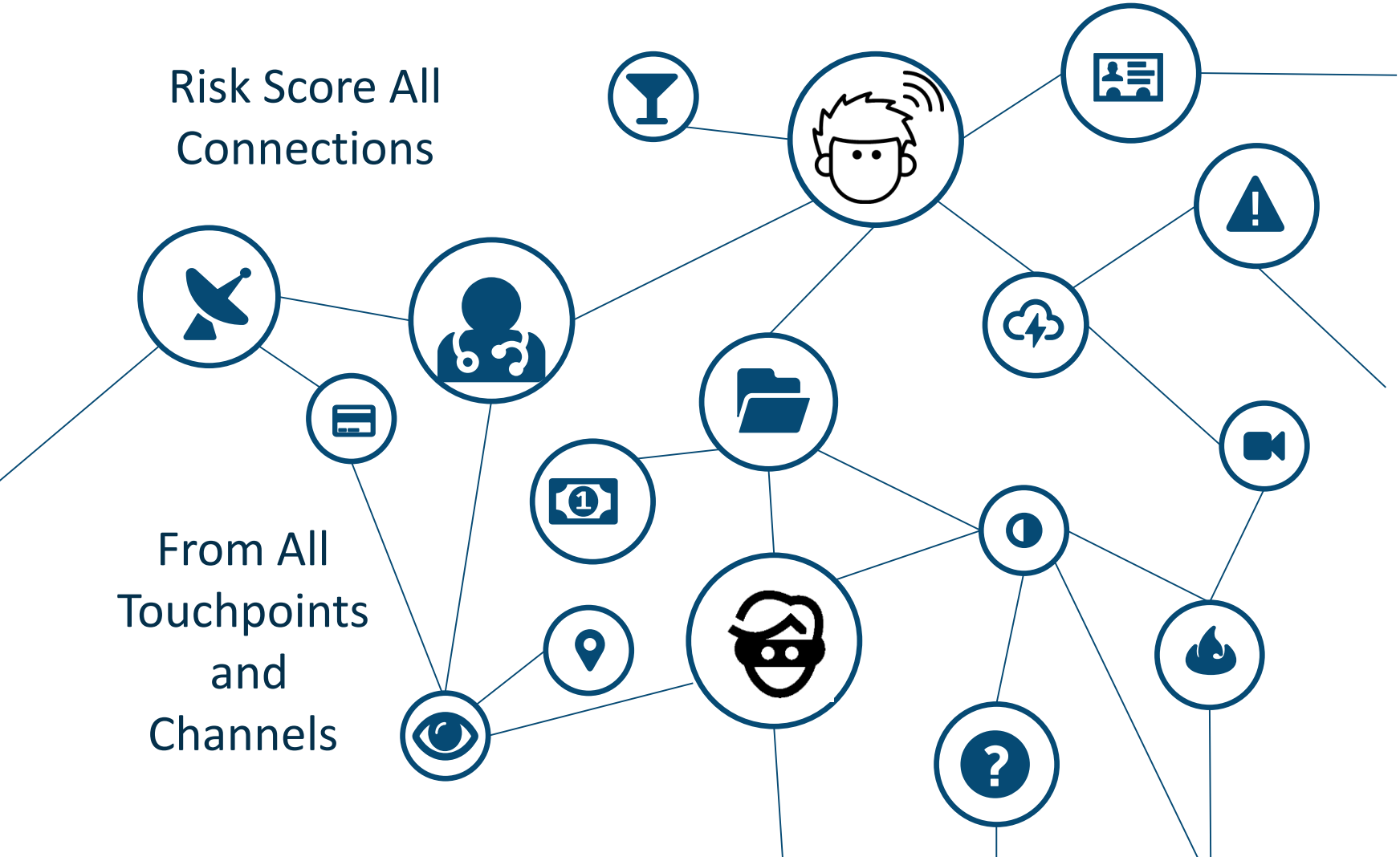
Transaction/Payment Monitoring

Debt Collection

And a Criminal-Centric View!

Risk Score All Connections

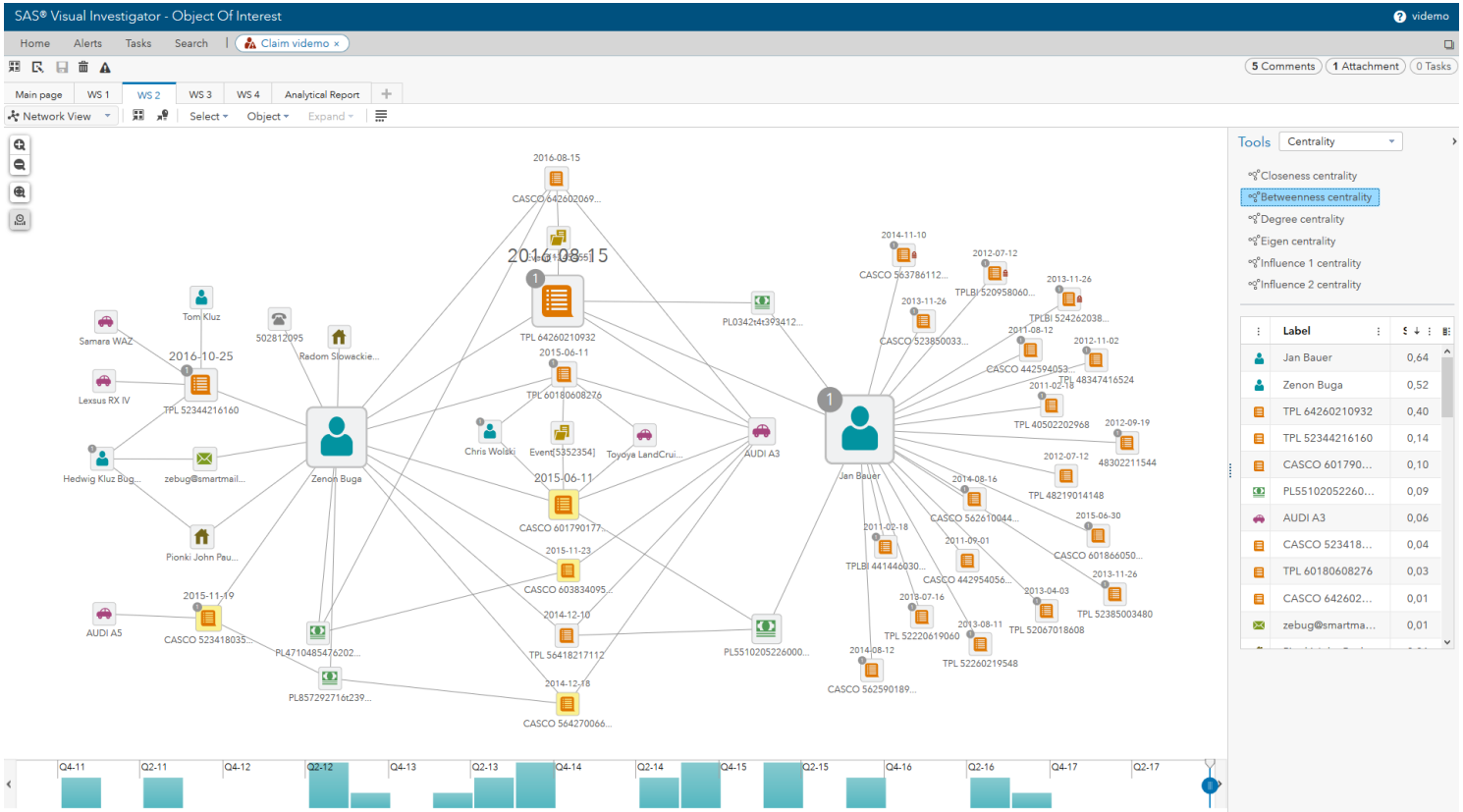
From All Touchpoints and Channels



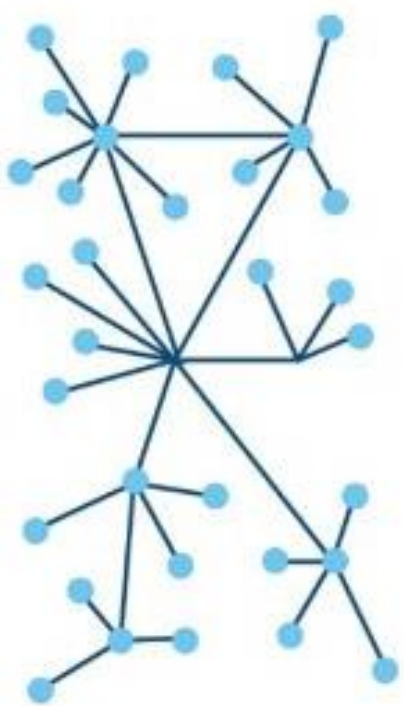
sas

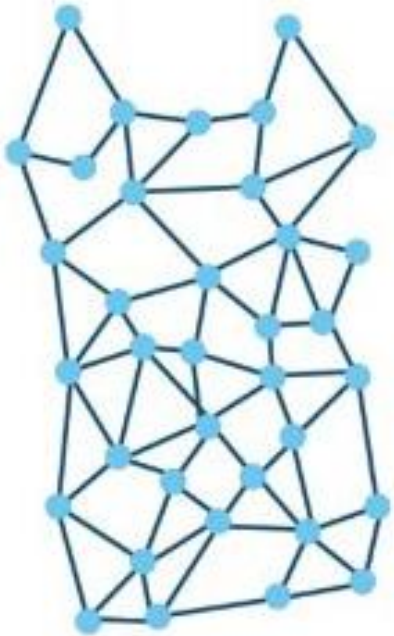
Network Analysis

Visualization & Discovery

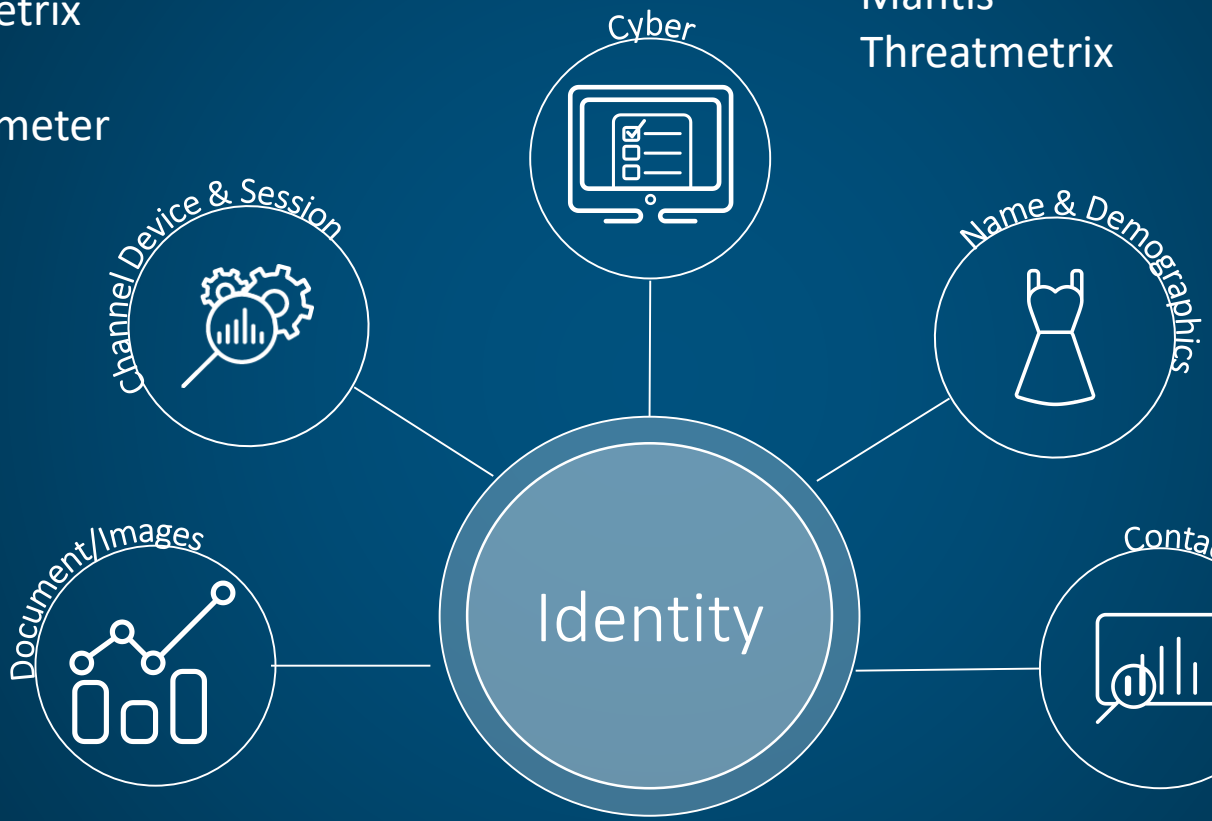


Growth in Digital Data





Sources



Threatmetrix
Iovation
41st Parameter
PinDrop
Socure

Mantis
Threatmetrix

LexisNexus
Equifax
Experian
BvD
HIS Markit
C6

Jumio
OnFido
Confirm.io

192.Com
Iovation
Nexmo
DigitalResolve
Emailage
Whitepages

Entities & Networks

Typical existing fraud systems

Event only alert

Event

e.g. account application

Attributes

e.g. loan amount

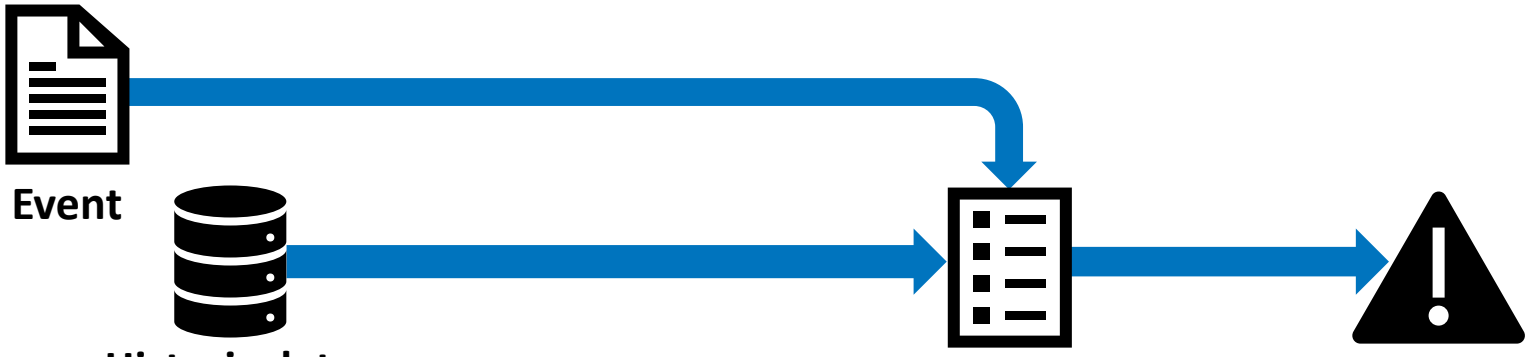
Alert

e.g. fraud risk

The simplest approach identifies/calculates some attributes from an event and then using a modelling approach to try and predict an outcome

Typical existing fraud systems

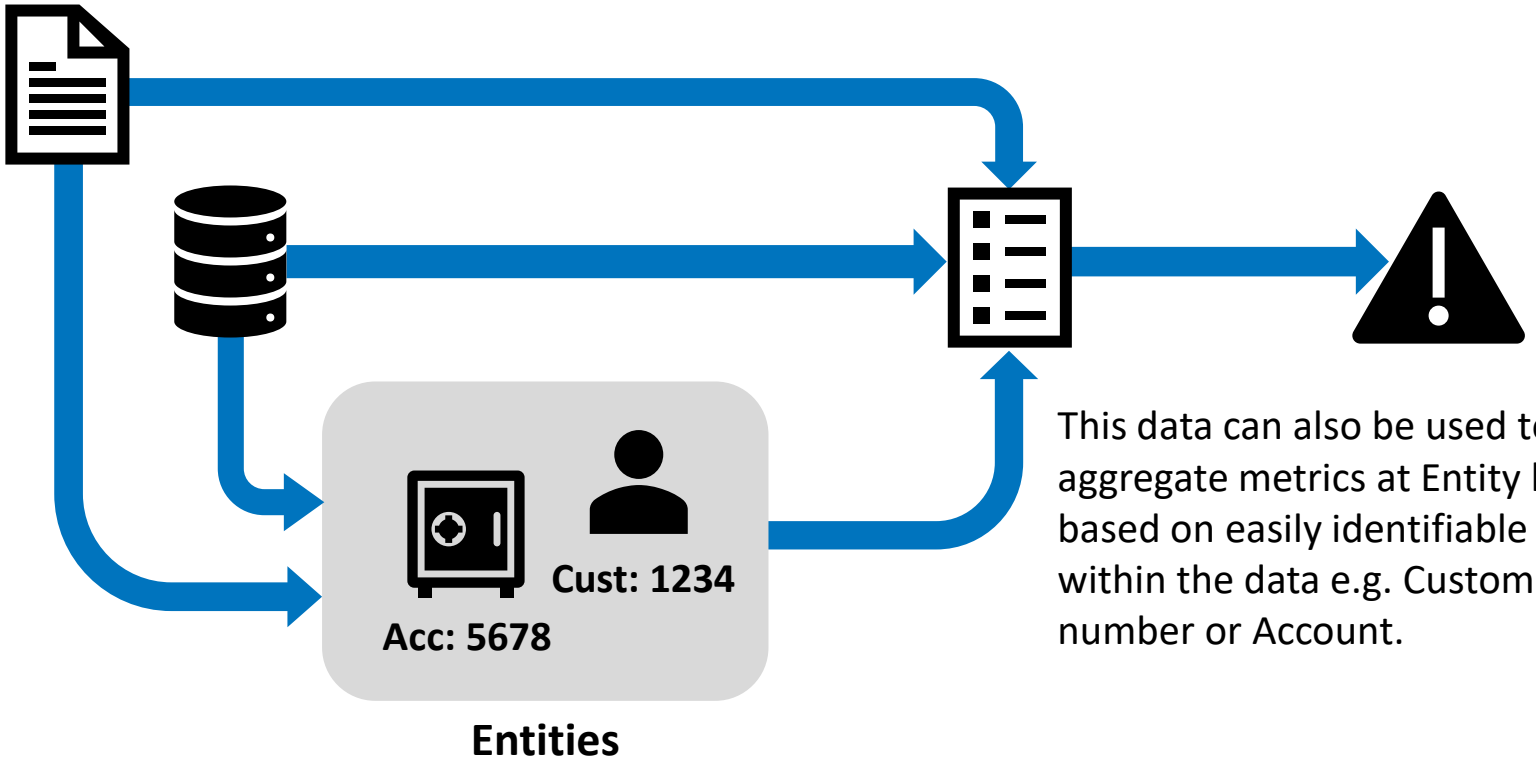
Event and historic data



In addition if additional customer data and historic data is available this can be used to add additional attributes and enhance the model

Typical existing fraud systems

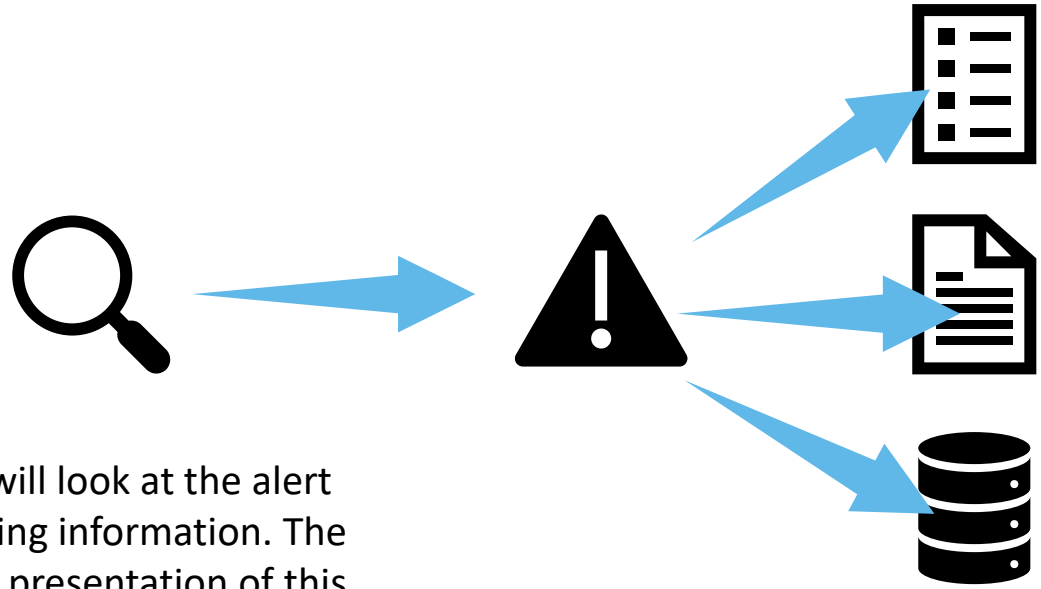
Aggregating at “Entity” level



This data can also be used to aggregate metrics at Entity level based on easily identifiable Entities within the data e.g. Customer number or Account.

How do investigators assess

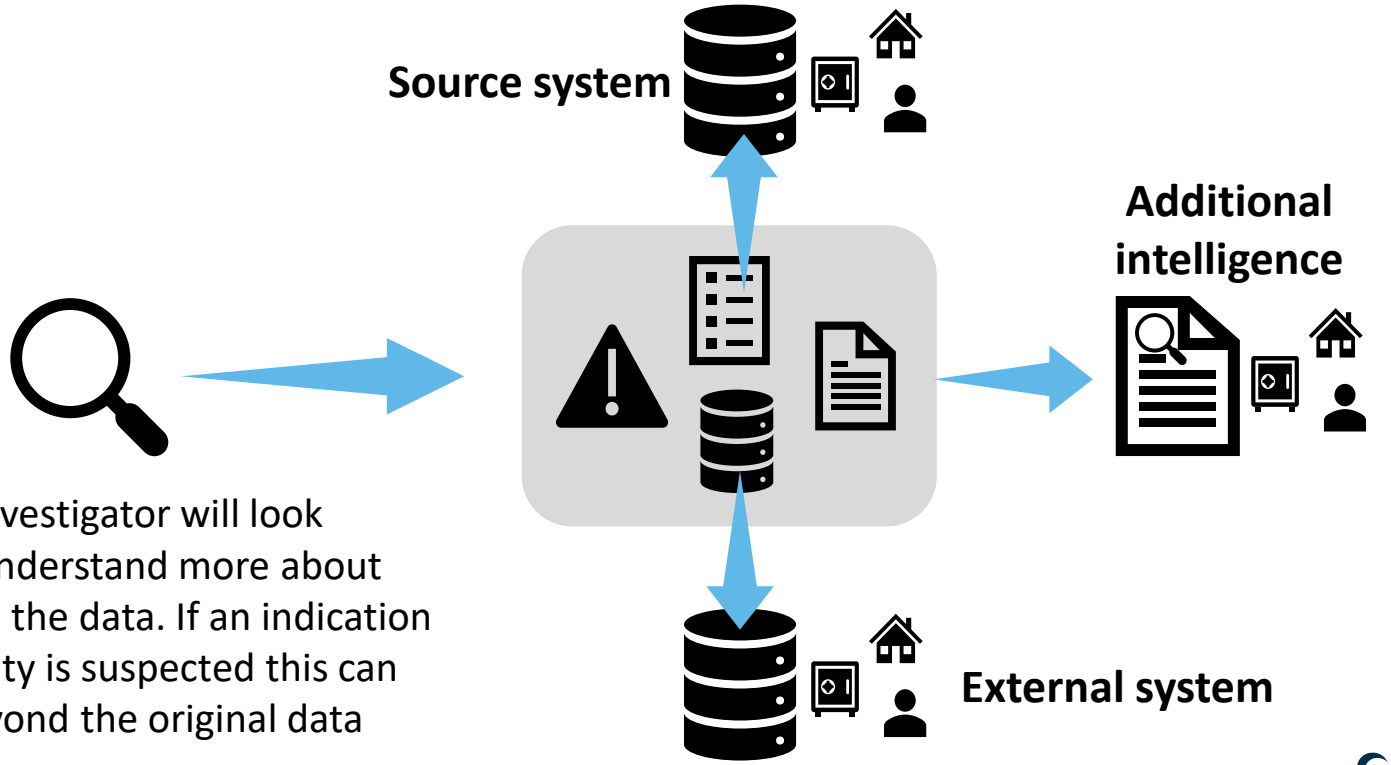
Study the alert and the supporting information



An investigator will look at the alert and the supporting information. The accessibility and presentation of this data ensures that the investigators can be thorough and efficient.

How do investigators assess

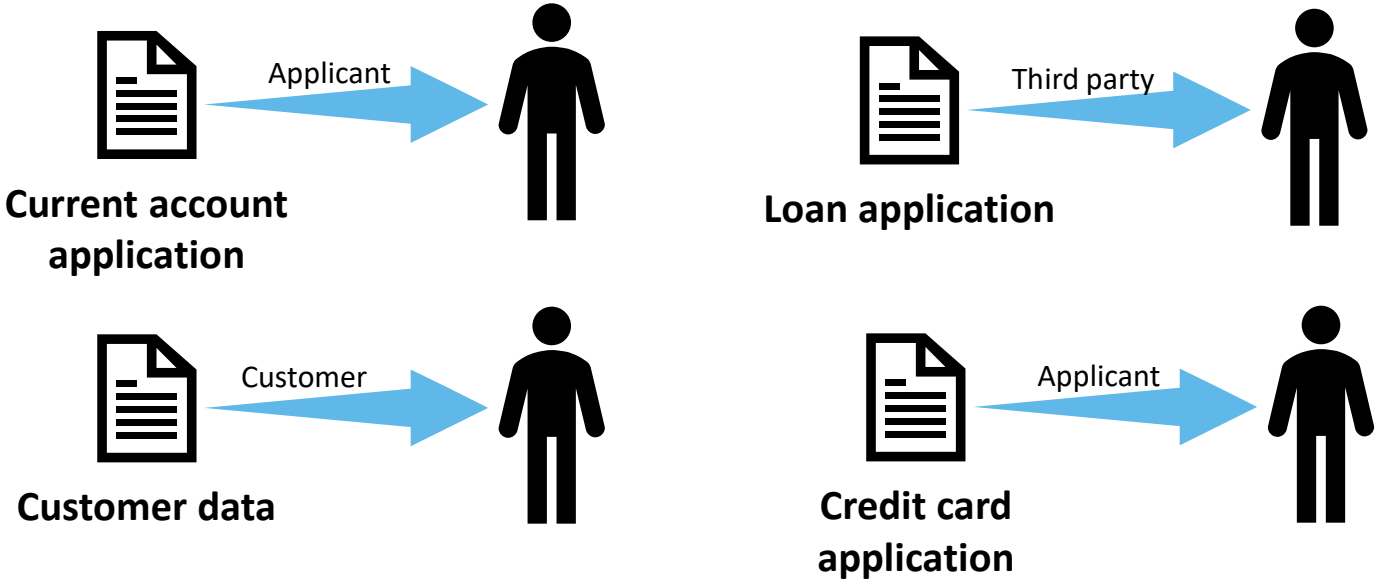
Manually extending the investigation



If necessary the investigator will look further afield to understand more about the entities within the data. If an indication of organised activity is suspected this can extend out far beyond the original data used for alerting

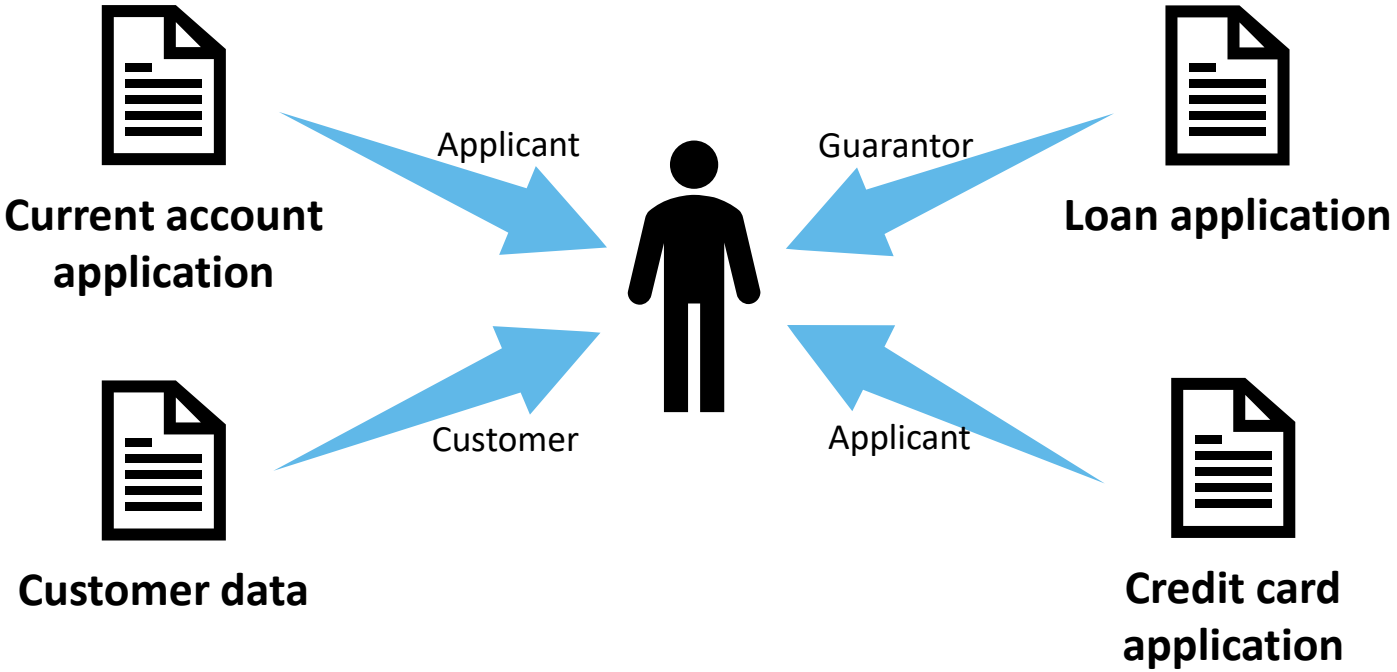
Resolving Entities

What does the bank see?



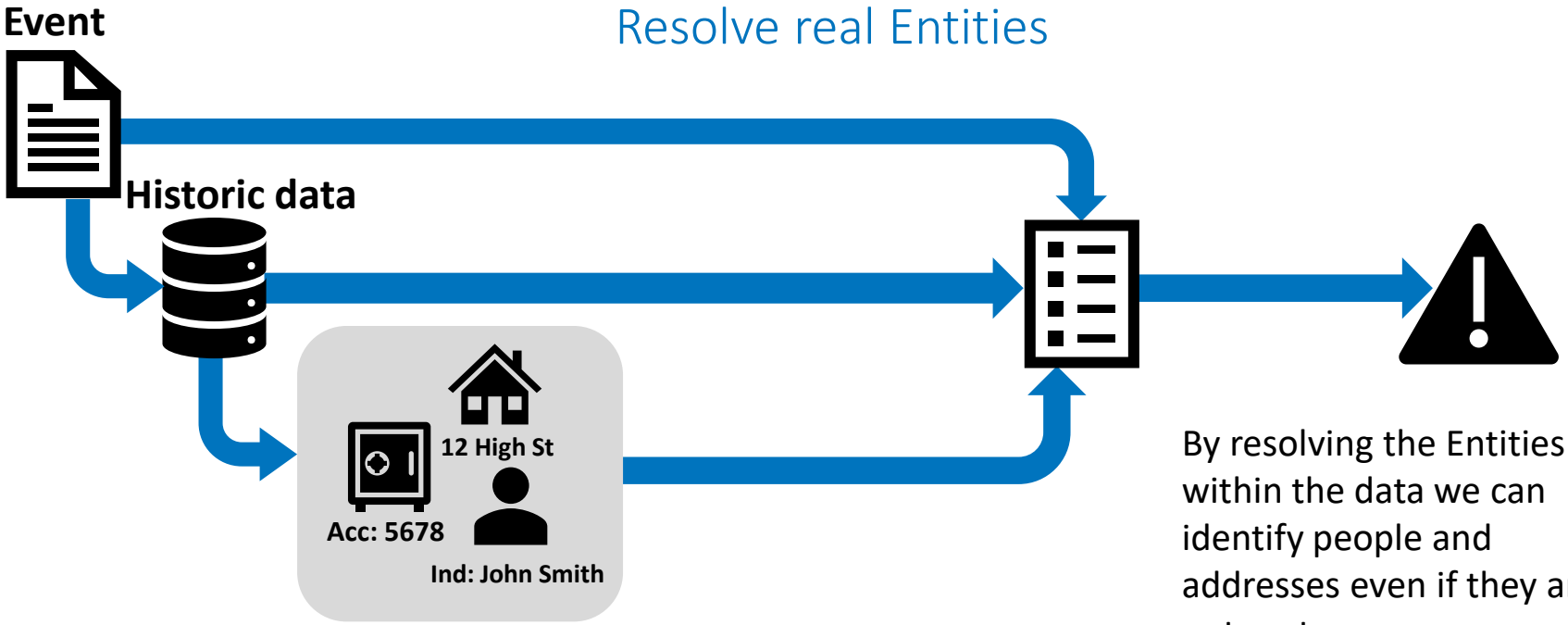
Resolving Entities

What is really needed



Entity resolution and Network analytics

Resolve real Entities



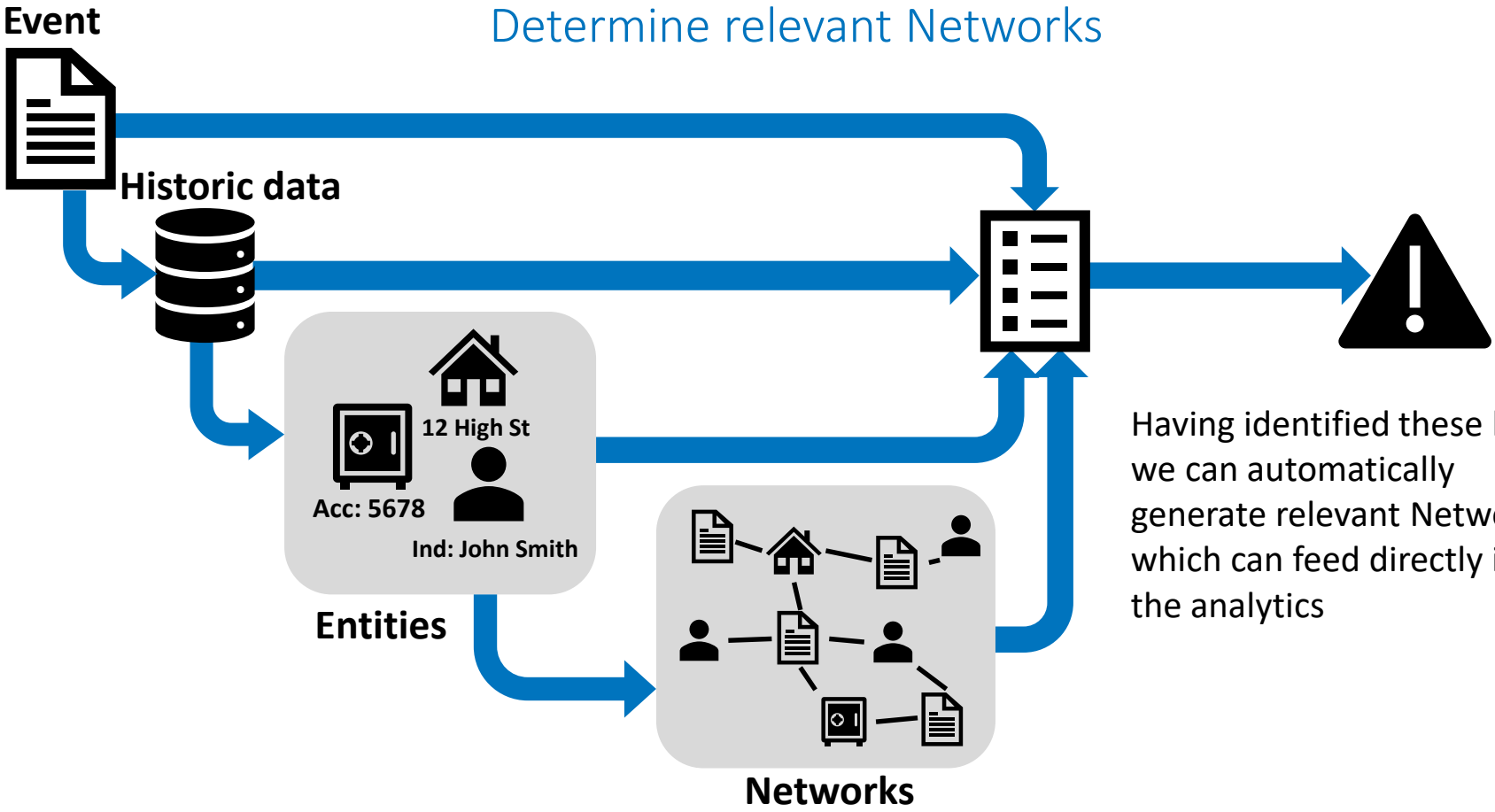
Entities

e.g. a person or an address

By resolving the Entities within the data we can identify people and addresses even if they are not customers

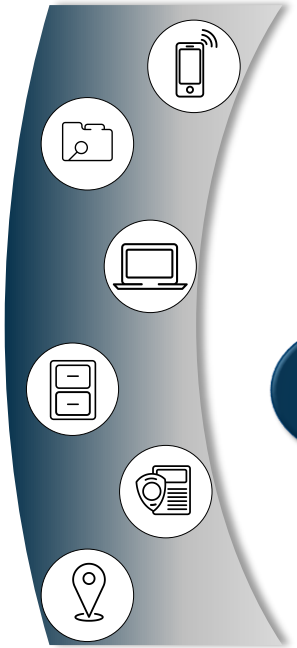
Entity resolution and Network analytics

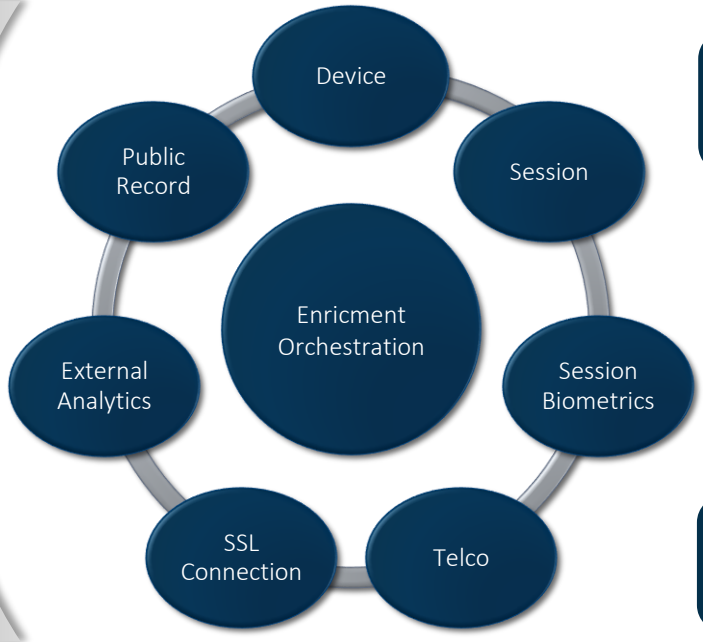
Determine relevant Networks



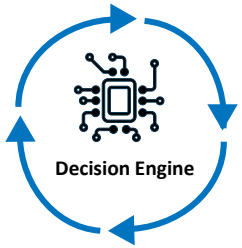
Having identified these links we can automatically generate relevant Networks which can feed directly into the analytics

Pillars to Success





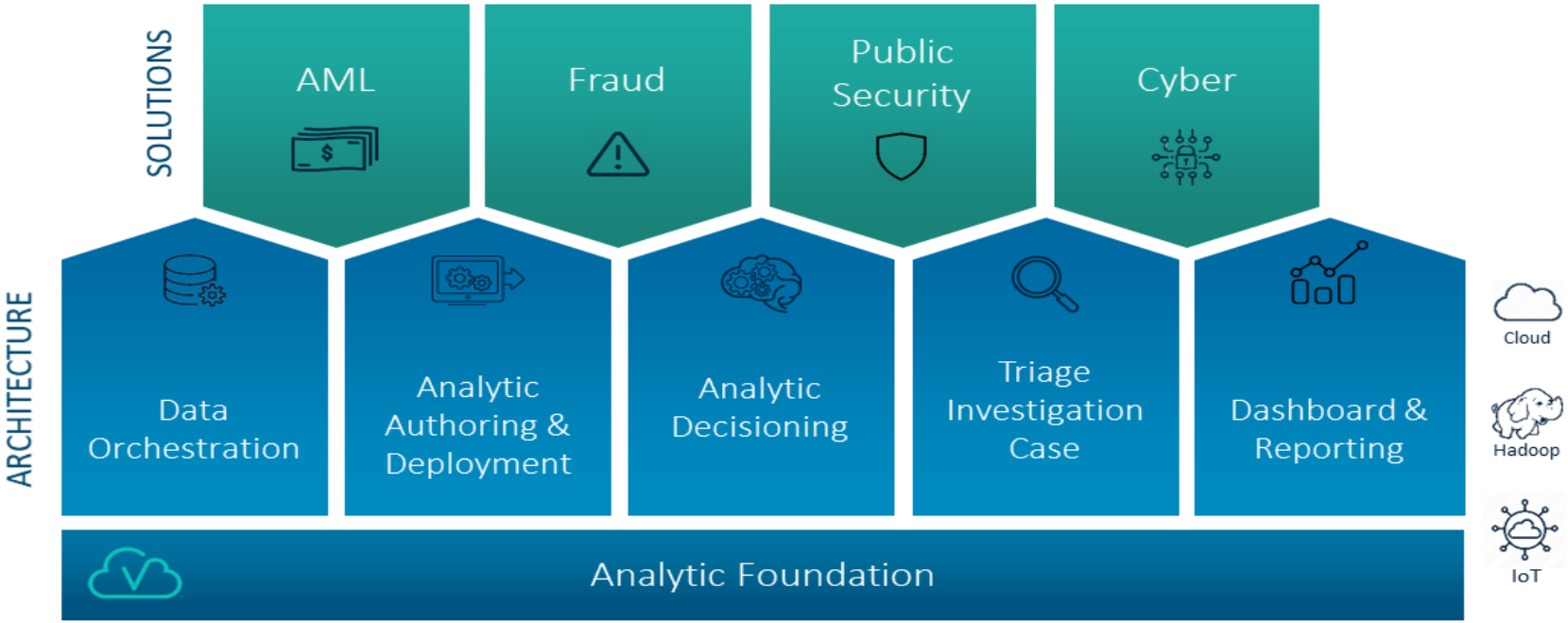
Machine Learning Models



Link Analysis

Fraud & Security Intelligence Analytic Architecture

Integration 2020



- **One platform across all F&SI solutions**
- **Ease of implementation for add-on solutions**
- **Consistent User Interface for triage and investigation**

Key Components Needed

Use all available data

Improve fraud detection

Integration layer

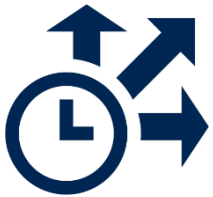
Significant saving in integration effort

Signatures

Holistic cardholder view

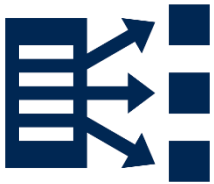
Advanced machine learning

Reduce false positives



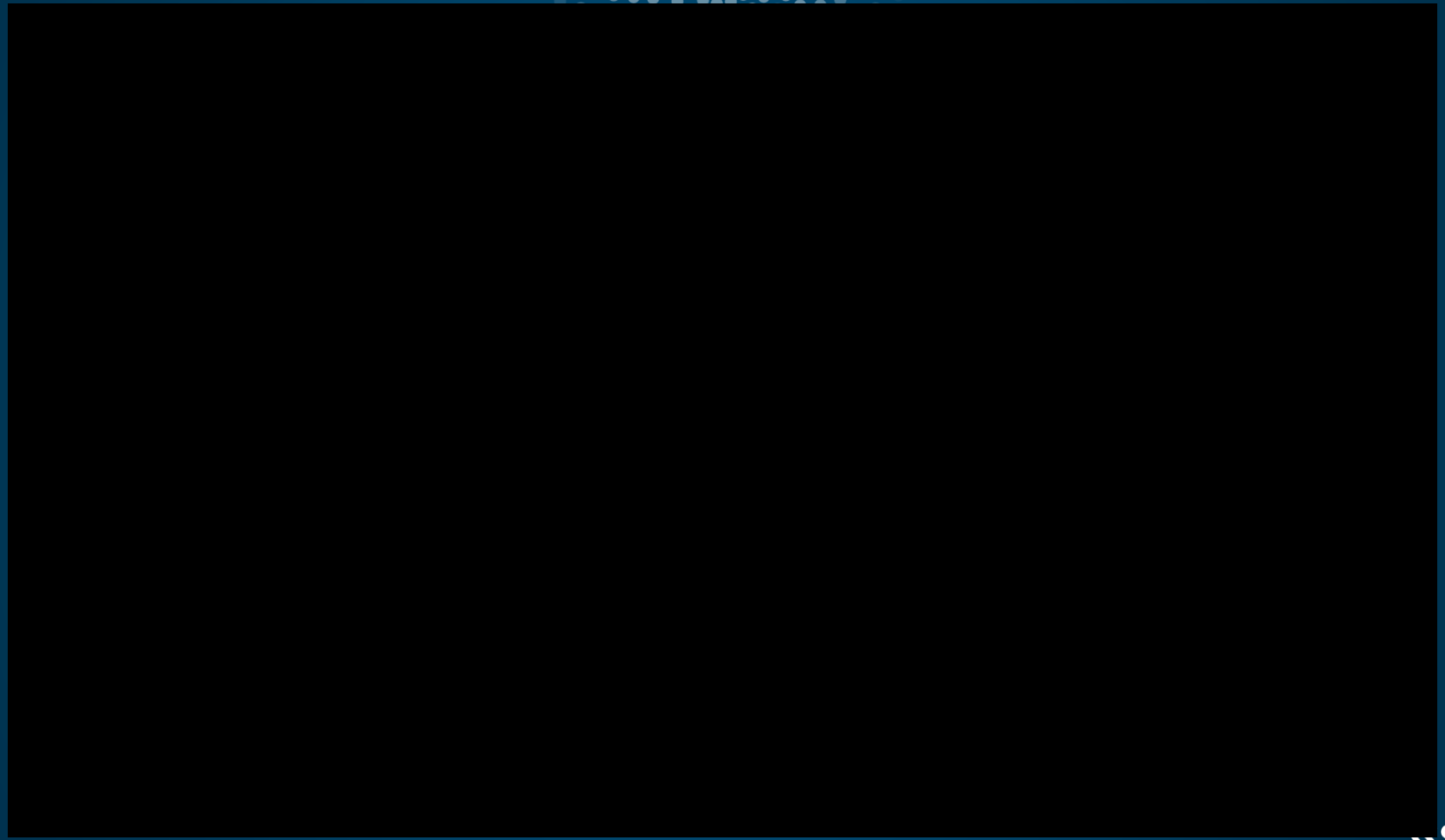
Real-time scoring

Stop fraud earlier

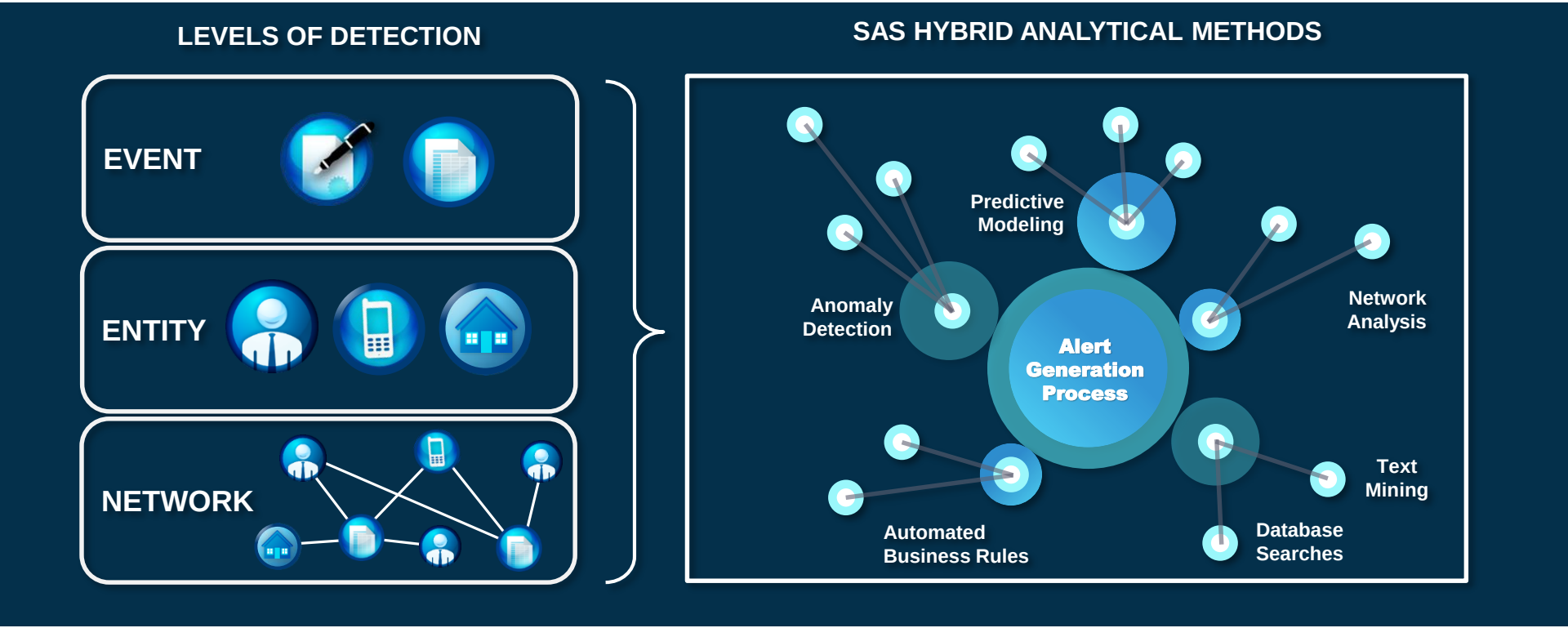


Rules writing capabilities

Flexible detection strategy



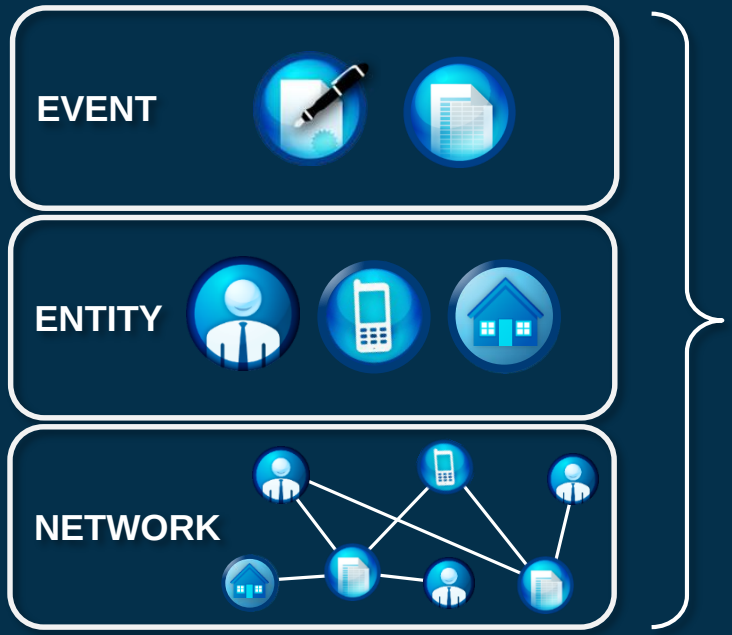
SAS Hybrid Approach for Detection



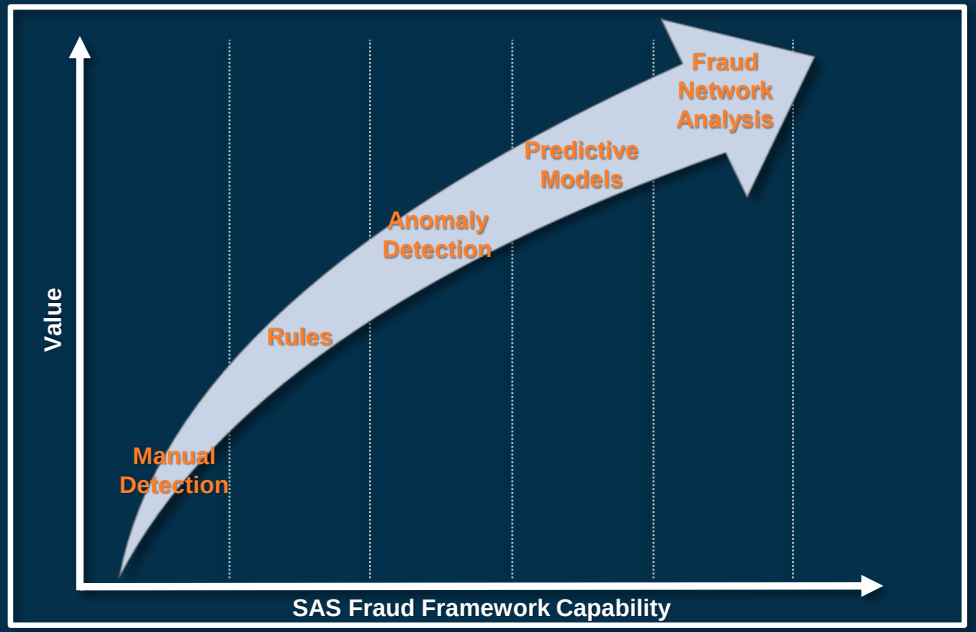
SAS Hybrid Approach for Detection

Improved accuracy & reduction of false positives

LEVELS OF DETECTION



SAS HYBRID ANALYTICAL METHODS

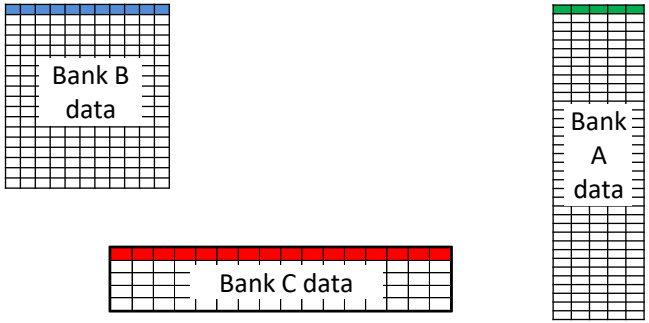


Two Approaches to Models

- **Custom model – analytics designed specifically for the client**
  - Typically maximises use of their own data but can have varying proportions of data from other banks (you may hear the term Hybrid)
  - Built in collaboration with client
  - Greater longevity
  - Can use bespoke data fields as well as transaction types
  - Rebuilt based on contract terms (c.18 months) or client performance
- **Consortium models - analytics designed to be suitable several clients**
  - Built by SAS to maximise suitability
  - Uses standard data fields and transactions
  - Rebuilt based on SAS timescales

Custom model

Bank A – large sized transaction volume with a small range of fields
Bank B – medium sized transaction volume with a wide range of fields
Bank C – small sized transaction volume with an extensive range of fields



Custom model can only use the clients fields to a maximum extent as we know we will receive them all in production.

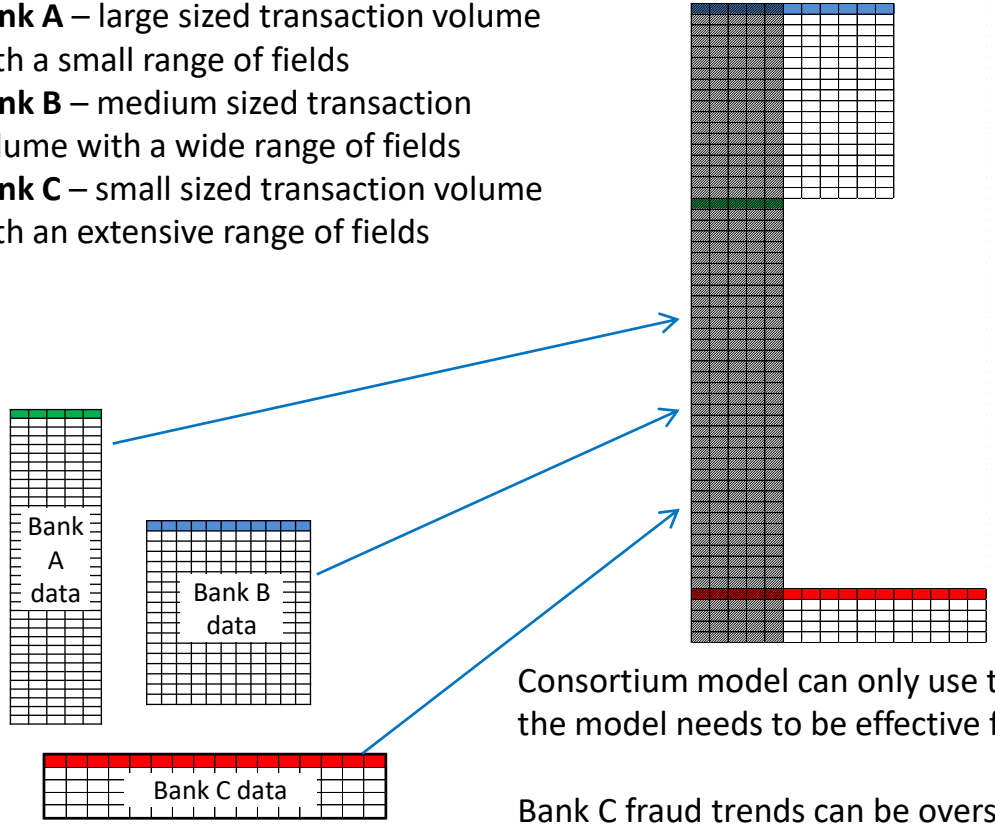
All could benefit from small portions of data from the consortium but do benefit from the modelling experience of the modelling team.

The fraud and genuine for each will be well represented.

Note: Bank C may not have sufficient data for a model in isolation.

Consortium model

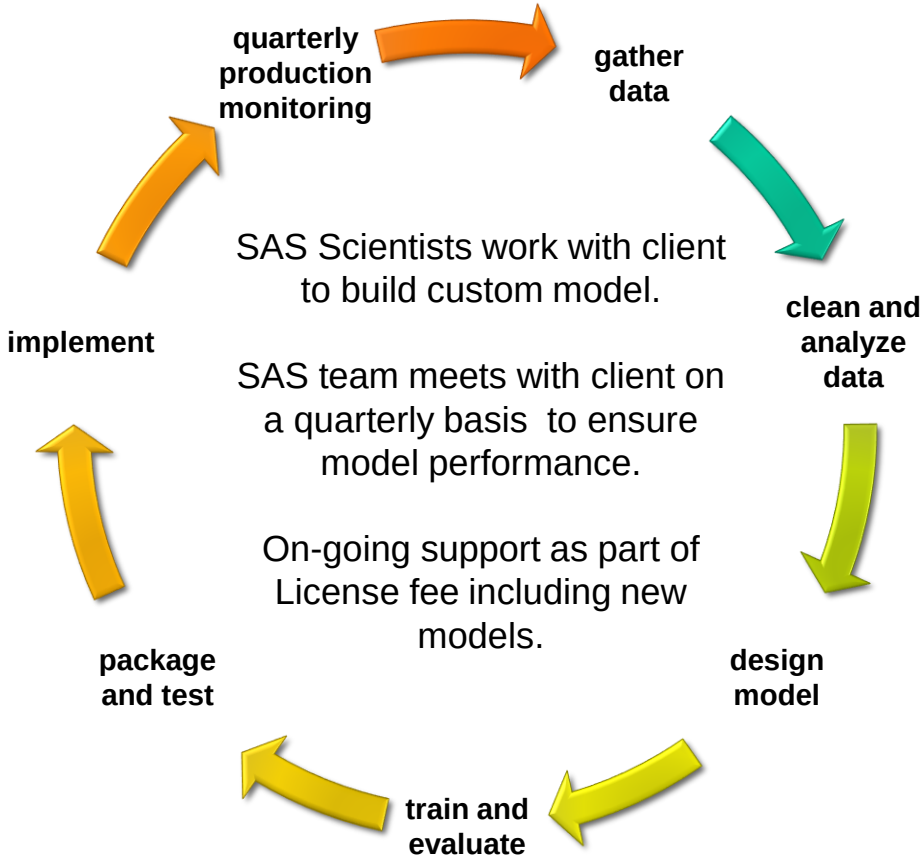
Bank A – large sized transaction volume with a small range of fields
Bank B – medium sized transaction volume with a wide range of fields
Bank C – small sized transaction volume with an extensive range of fields



Consortium model can only use the common fields as the model needs to be effective for all clients.

Bank C fraud trends can be overshadowed

Typical Development Stages



Online Fraud – Example Scenarios

Online Fraud Scenario 1

Situation

Multiple failed logins followed by multiple payments to new beneficiaries

Solution

Added risk for transactions following this type of behaviour

Comment

This type of behaviour alone may not be sufficient to trigger an alert

Online Fraud Scenario 2

Situation

New beneficiary set up from black-listed device

Solution

Block any subsequent transactions over a certain threshold

Comment

Black-listed device can be replaced by any watch-list item

Online Fraud Scenario 3

Situation

Savings account 'emptied' and transferred to new beneficiary

Solution

Added risk (score) after a big me2me transaction from a savings account

Comment

Based on the percentage of savings spent in the same session or the value. Can also leverage peer group information to complement historical profile data.

Online Fraud Scenario 4

Situation

Multiple payments in short time to a suspicious location

Solution

Added risk (score) for all transactions to this location

Comment

This allows the bank to quickly react to new trends and 'modus operandi'.

This could be based on a the last hours worth of transactions.

Online Fraud Scenario 5

Situation

Customer has set up a new beneficiary that is to a known internal or external mule

Solution

Block current and any subsequent transactions pending investigation

Comment

This type of behaviour alone may not be sufficient to trigger an alert but would be a strong risk contributor.

And the ‘AI’ Part?

What is Artificial Intelligence?

Artificial intelligence is the science of training systems to emulate human tasks through Learning and Automation

Copyright © SAS Institute

What is Machine Learning?

Machine Learning is a branch of artificial intelligence based on the idea that systems can **learn from data**, **identify patterns** and **make decisions** with minimal human intervention.

What are we and machines good at?

US

GOOD AT

COMMON SENSE

INTUITION | CREATIVITY

EMPATHY | VERSATILITY

MACHINES

GOOD AT

LARGE DATA SETS

COMPLEX CALCULATIONS

LEARNING | AUTOMATION

Copyright © SAS Institute Inc. All rights reserved.

What are we and machines good at?

US

+

MACHINES

Machine learning enhances our capability and gives organizations competitive advantage

Copyright © SAS Institute Inc. All rights reserved.

Machine Learning can improve predicting accuracy
and maximize optimization by leveraging hidden patterns in data

Improved prediction adjustment

Recognize hidden patterns in data

Improve productivity of prediction

Improved operations by prediction

Copyright © SAS Institute Inc. All rights reserved.

Copyright © SAS Institute Inc. All rights reserved.

4 A's of AI

Automation, Accuracy, Adaptability & Accountability

Automation

Key to reducing the decision lag (the time between observation and action), maximizing system effectiveness.

Accuracy

A function of problem definition, data engineering, breadth of supervised and unsupervised algorithms and best practices.

Adaptability

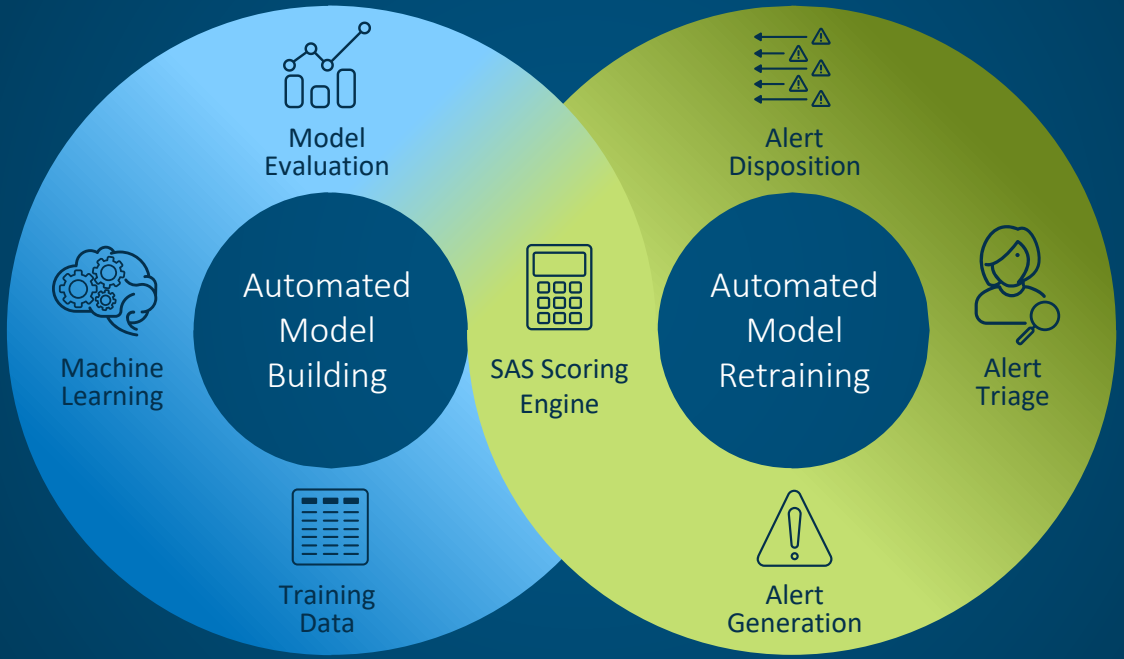
Learning new and emerging patterns and threats within the data, minimizing detection lag, minimizing or eliminating model degradation overtime.

Accountability

Consistency, interpretability, and governance of the system. Produce interpretable results, digestible by both the business and layman.

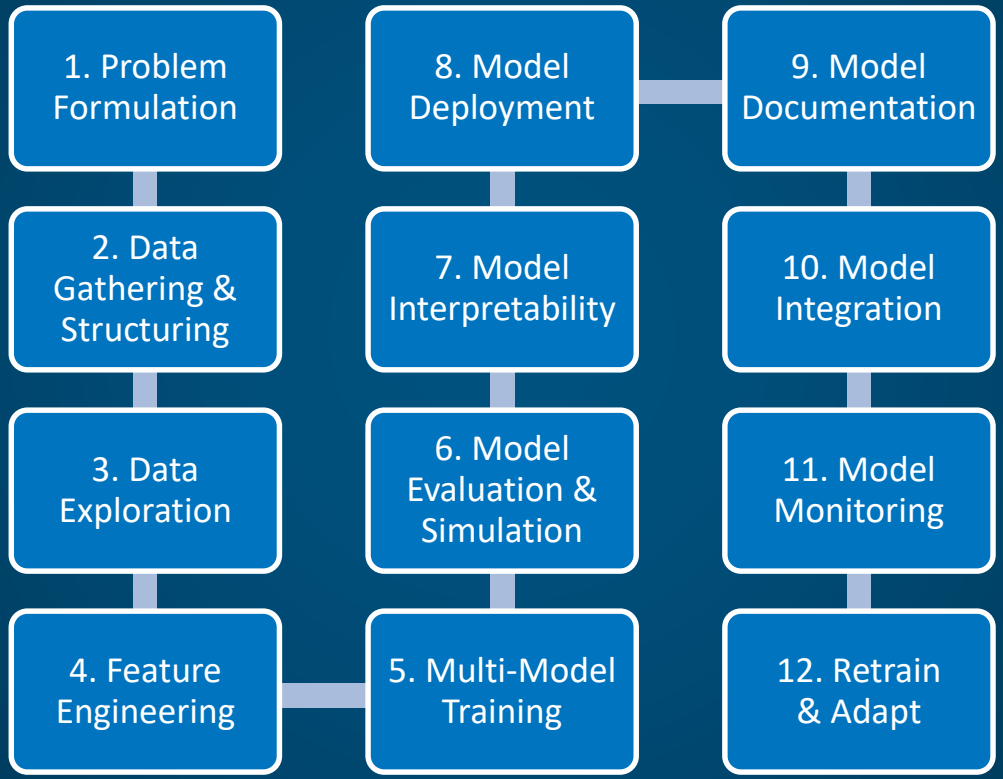
Automated Model Building and Retraining

Adaptive Learning



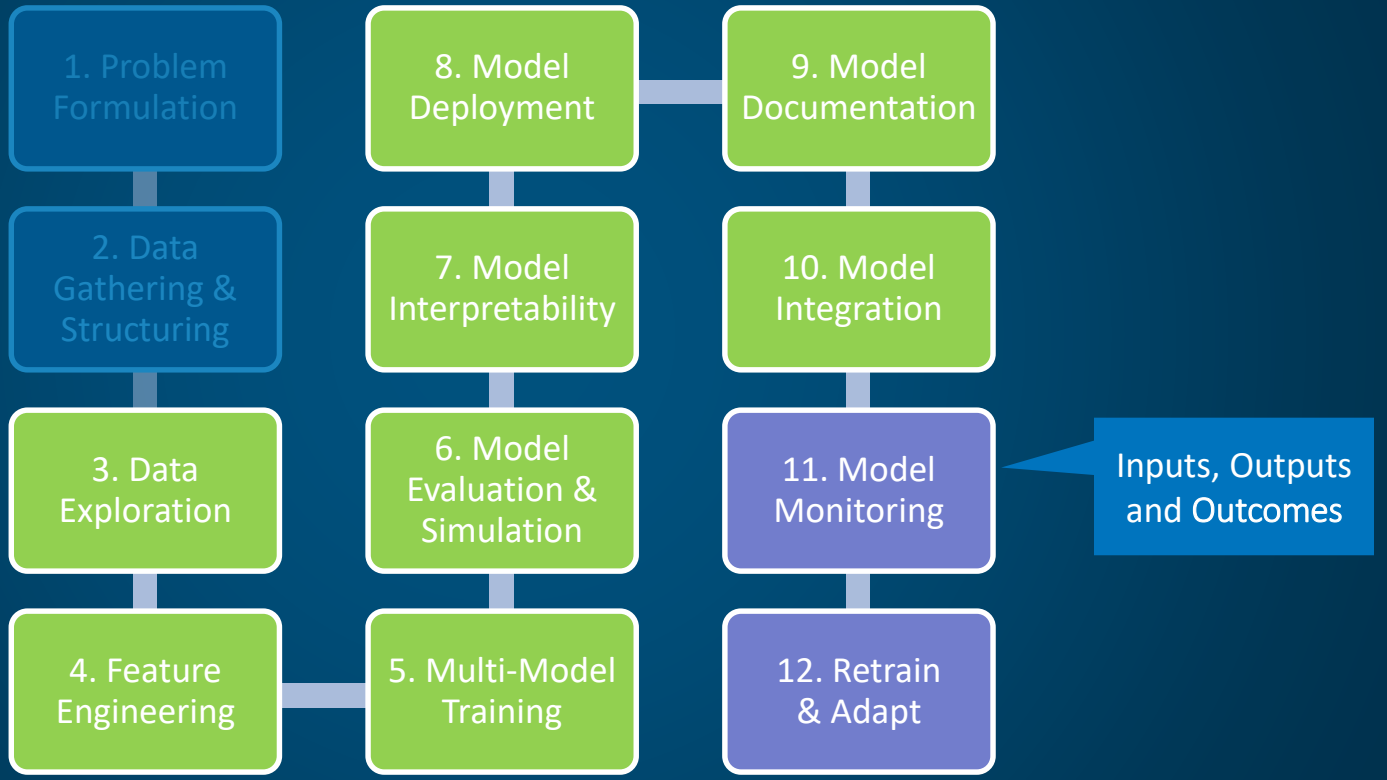
Typical Flow

Problem Definition, Model training, Integration to & Monitoring

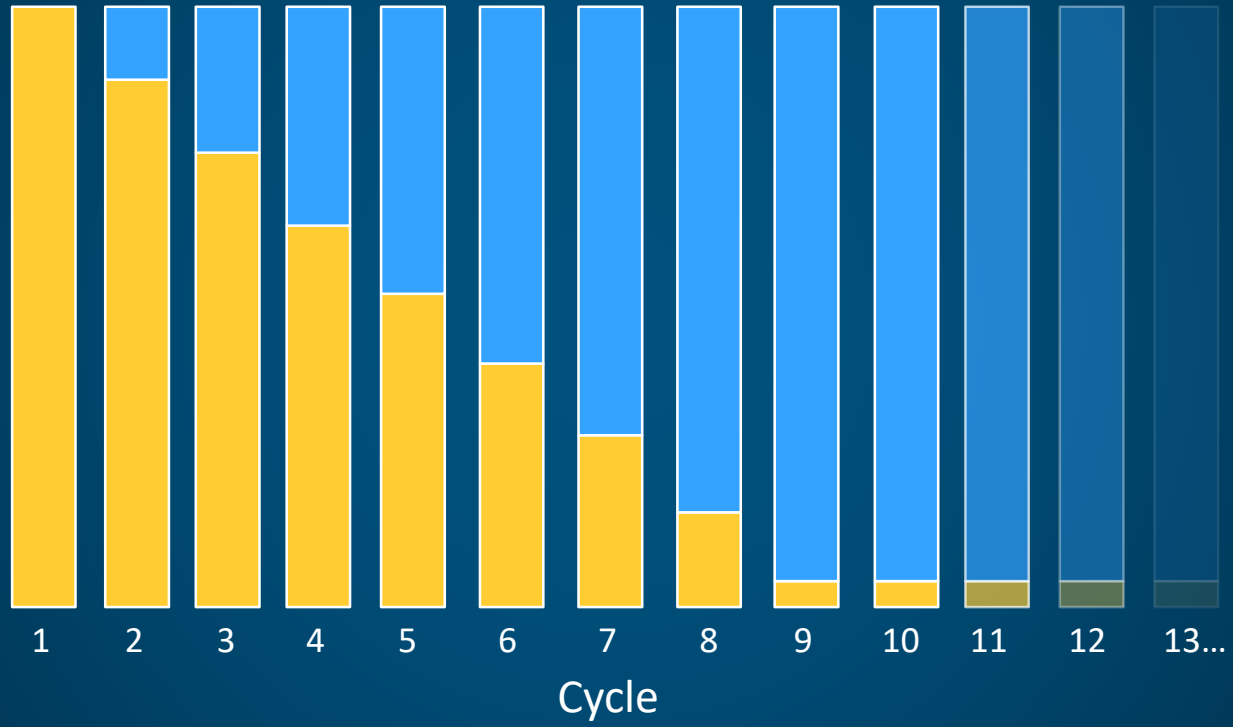


Typical Flow

Automate the key pieces & do as much as possible in real-time



Transition from Unsupervised to Supervised Learning



What Does It Look Like?

Demonstration

Summary/Conclusion

What does this all mean?

1. In order to get a ‘Criminal-centric View’, advanced and fast entity resolution and automatic network generation is vital, across all channels and **‘touchpoints’**
2. Not just the customer behavior but ALL entities relating to the customer should contribute to the fraud risk scoring process
3. Machine Learning Models & AI is vital to embrace the scale and complexity needed whilst also constantly learning new behavior and re-scoring at the speed needed to prevent financial crime

IN YOUR LANGUAGE - it helps….

Reduce false positives, increasing channels, volumes & risk

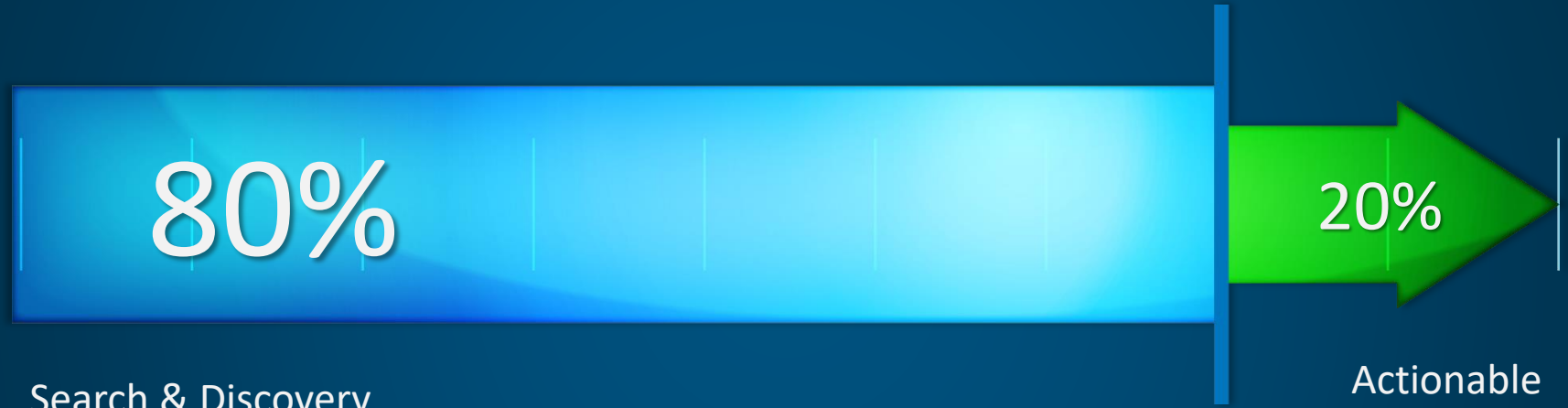
“Faster payments” moves settlements to real-time

Automation of manual processes aka “Robotic Process Automation”

Regulatory scrutiny and transparency – know your customer and your risk

Pressure to use Artificial Intelligence & Machine Learning

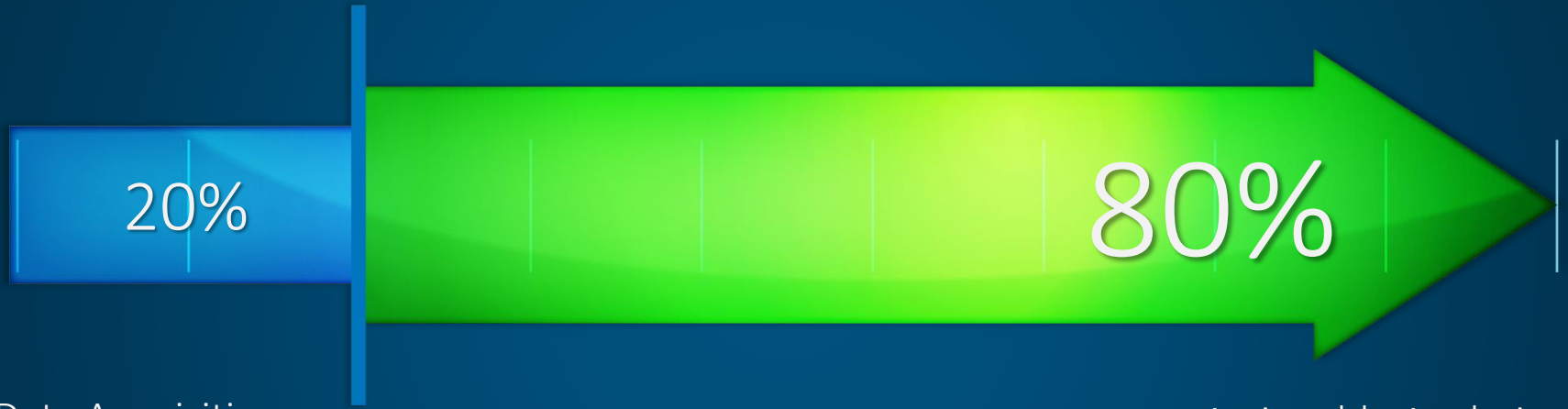
Remember This?



Search & Discovery
Labour intensive: Identifying relevant information, searching various data sources, “formatting” data for a specific tool, processing, applying “analytical techniques” within a tool, typically ad-hoc and manual.
OFTEN TOO LATE TO PREVENT IT

Actionable Analysis
Applying specific tradecraft, vetting of information

Operationalised with Advanced Analytics



Data Acquisition, Integration, & Automated Analytics

Actionable Analysis

More time to look at High Value Targets and the most impactful information to the organization

*Analytics informs on targets to be reviewed

Thank You

gerard.mcdonnell@sas.com