# Local Partner in Financial Crime & Compliance

Trusted ▪ Proven ▪ Always Innovating


WE STOP
BAD PEOPLE
FROM DOING
BAD THINGS
REAKING NEWS:
N TRAFFICKING RING BU
RIST FINANCING

# BY USING

- WORLD CLASS ANALYTICS TOOL
- MACHINE LEARNING
- FACE BIOMETRY
- BEHAVIORAL ANALYTICS

# DVA Bilgi Teknojileri A.S. Istanbul

- Local Consultancy and Implementaion Resources for Fraud Monitoring and AML Solutions
- Implementation and Consultancy Experience since **2012**
- Experienced team about Turkish Regulations
- www.featurespace.com

# DVA Bilgi Teknojileri A.S. Istanbul

- Face Biometry Solutions for Mobile Bnaking
  - Customer log-in to mobile banking portals
  - KYC- mobile customer on-boarding
  - Uses deep learning to train the face matching engine

  - www.aware.com

AWARE

# DVA Bilgi Teknojileri A.S. Istanbul

- Behavioral Biometrics Solutions for banks against Fraud
- Profile Mouse, key stroke, finger movements, pressure and all device realted information for each user by using machine Learning
- www.behaviosec.com

BehavioSec

# WORLD CLASS ANALYTICS

# WITH LOCAL EXPERIENCE


DVA BİLGİ TEKNOLOJİLERİ A.Ş.

WWW.DVA.COM.TR

GOKHAN.GOZUTOK@DVA.COM.TR

GSM: 0532 213 63 47


DATA VIDEO AUDIO

# Bankacılıkta Yaşanan Güncel Suistimal Vakaları ve Trendleri

**21 KASIM 2019**


## Erhan ATEŞ

Türk Ekonomi Bankası A.Ş.

Suistimal Önleme, Tespit, Analiz ve Geliştirme Birim Yöneticisi

Sunumda anlatılan vakalar,
sadece TEB A.Ş.ye ya da sadece spesifik bir kuruma ait olmayıp Türkiye'de ve dünyada yaşanan gerçek vakalardan derlenmiştir.

# INTERNAL – EXTERNAL FRAUD

**İç dolandırıcılıklar**

- Sıfır tolerans politikası
- İtibar kaybı
- Müşteri kaybı
- Müşteri deneyimi 2.planda
- Bildirim ve raporlanma

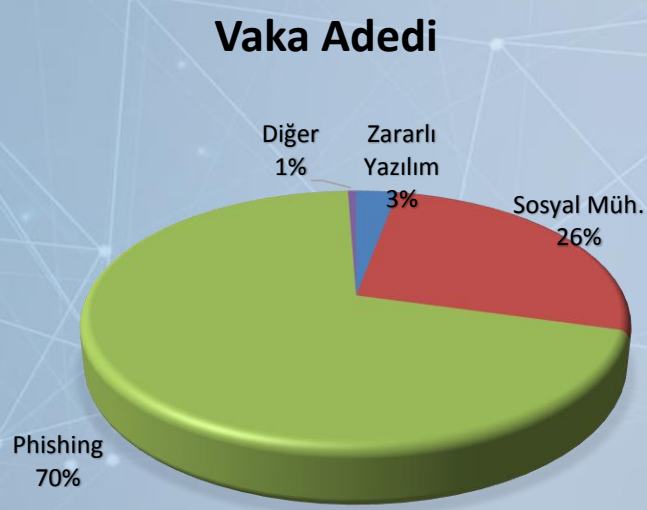
**Dış dolandırıcılıklar**

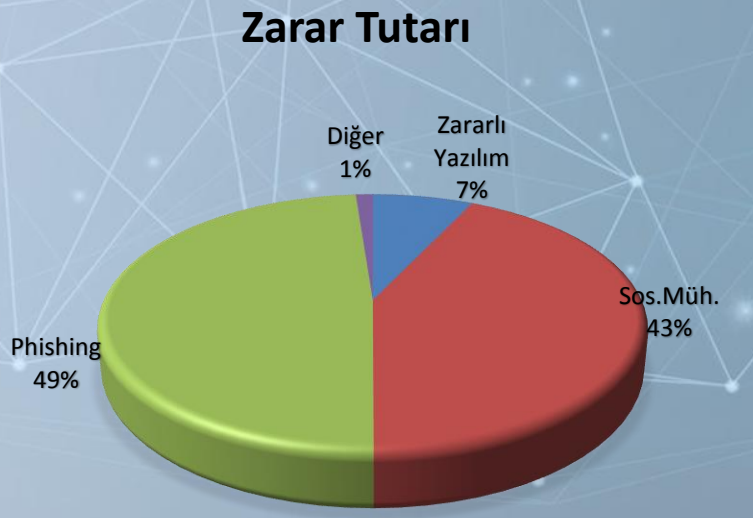
- Tolerans eşiği yüksek
- Yüksek risk iştahı / Müşteri deneyimi
  - İşlemin reddedilmesi
  - İşlemin askıya alınması
  - Telefon/SMS ile işlem teyidi
- Daha şeffaf raporlama

# INTERNAL – EXTERNAL FRAUD

# EXTERNAL FRAUD

## DOLANDIRICILIK TİPLERİ

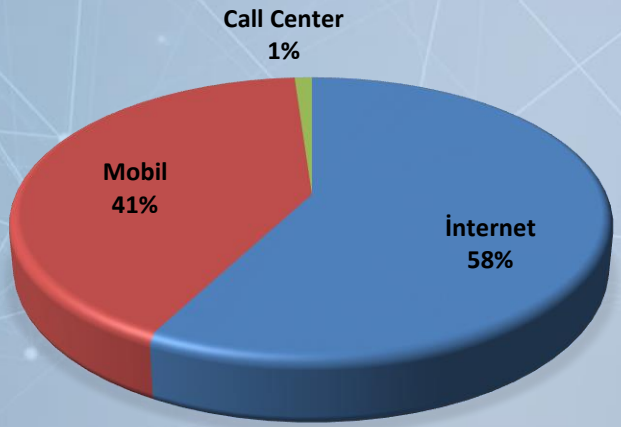


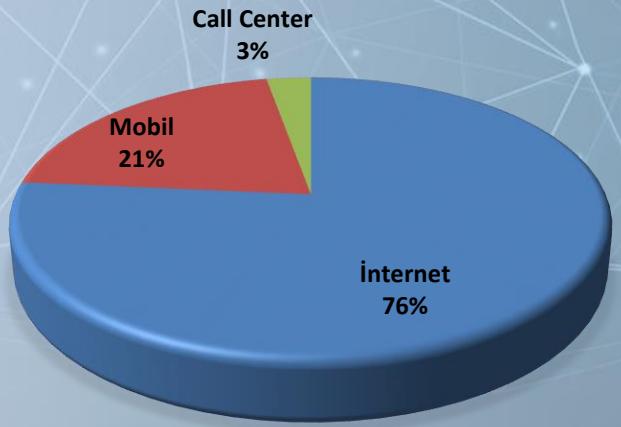
# EXTERNAL FRAUD

## KANAL TİPİNE GÖRE DAĞILIM

### Vaka Adedi




### Zarar Tutarı



# SIM KART DOLANDIRICILIKLARI

*Afrika'da yılda 150 mio USD kayıp*
*Brezilya'da 5.000 adet vaka*

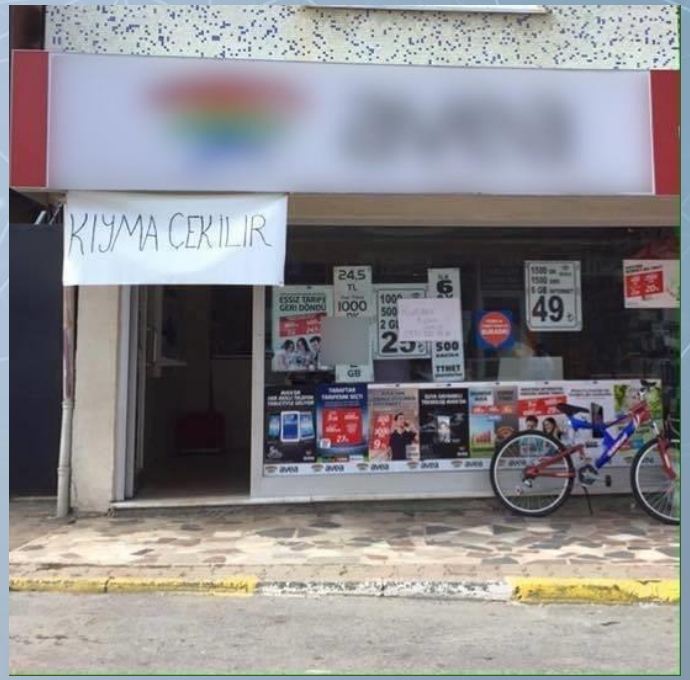
- Sahte kimlik ile operatörden sim kart temini
- Gerçek müşterinin hattının kesilmesi
- Bankacılık ve kart şifrelerinin ele geçirilmesi
  - sahte çağrı merkezi
  - phishing siteleri
- Ele geçirilen şifreler ile sim kart blokesinin kaldırılması

# SIM KART DOLANDIRICILIKLARI

**BANKALAR**

47 banka
4,3 trilyon TL aktif büyüklük
10 bin şube
190 bin çalışan

**GSM BAYİLERİ**



# SIM KART DOLANDIRICILIKLARI

## OPERATÖRLERİN SORUMLULUKLARI VE ÖNLEMLER

- Doğrudan fotokopi kimlik ile işlem yapılması
- Kimlik üzerindeki güvenlik kontrollerinin yerine getirilmemesi
- Merdiven altı GSM bayileri
- Eğitim yetersizliği

- eSIM teknolojisi
- Uyarıcı mesajlar
- Ek güvenlik soruları
- Aktif telefona SMS
- Mevcut kimliğin eşleştirilmesi

# SIM KART DOLANDIRICILIKLARI

## BANKALARIN SORUMLULUKLARI VE ÖNLEMLER


- Güvenlik akışlarının gözden geçirilmesi
- 90 günlük sim kart blokaj yapısının verimli kullanılması
- Müşterinin “bildiği” faktörler yerine “sahip olduğu” ve “kendisinin olduğunu” ispat edecek faktörlere yönelinmesi

# PHISHING SALDIRILARI

## Sahte/Taklit Web Sayfaları


- Bankalar
- E-devlet / Turkiye.gov.tr
- Kamu Kuruluşları
- Oteller
- Alışveriş siteleri
- Tüvtürk
- Vb.

# PHISHING SALDIRILARI

BTK/USOM'un acil aksiyonları ve proaktif çözümleri

Bankaların cihaz tanıma teknolojilerine yönelmesi

- Cihaz ID
  - IOS ID
  - Advertising ID
  - IMEI
  - Push Notification ID
- Konum
- IP
- OS versiyon
- Çözünürlük ve ekran boyutu
- Dil ayarları
- Zaman dilimi
- Tarayıcı tercihleri
- Parmak izi, Yüz tanıma
- Klavye yazma hızı
- Tuşa uyguladığı basınç
- Batarya seviyesi

# Çipli kimlik kartlarda NFC doğrulaması


- Şubelerde bizzat chip/NFC kontrolü
- Uzaktan/mobil cihaz üzerinden NFC aracılığıyla doğrulama
  - Fotoğraf
  - Kimlik bilgileri
- Uzaktan kredi başvurusu
- Mobil bankacılığına login, riskli işlemlerde kontrol

- Mobil cihazdan çekilen fotoğrafta canlılık kontrolü

# TELEFON / ÇAĞRI MERKEZİ DOLANDIRICILIKLARI

1. Müşterinin telefonun numarasının taklit edilerek banka çağrı merkezinin aranması
2. Banka çağrı merkezi numarasının başına farklı no ekleyerek müşterinin aranması
3. Bankadan gönderiliyormuş izlenimi verilen toplu SMS gönderimleri/Zararlı yazılım
4. Müşterilerin telefon numaralarının yönlendirilmesi

# BIN ATAKLARI

**SİBER SALDIRILAR – VISA/MASTERCARD DA ALARMDA**

Saniyeler içerisinde 10 binlerce kredi kartına sahte işlem

- Aynı BIN, aynı 12 hane
- MoTo ya da non secure E-com işlemi
- Aynı son kullanma tarihi
- CVV2'siz

- Kart üretim algoritmaları
- Vade tarihleri
- Otorizasyon engelleri

# VERİ SIZINTILARI

Şirketlerde kullanılan;

- Programlara, menülere,
- Raporlama ve
- Veri tabanı sorgulama araçlarına

ilişkin;

- denetim loglarının ve
- erişim istatistiklerinin tutulması,
- anlık olarak yaşanan anomalilerin takip edilmesi,
- DLP araçlarının kullanılması

büyük önem arz etmektedir.

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

# ATM LOGICAL ATAKLARI

- Kart kopyalama cihazları
  - Alarm üreten aparatlar ve yazılımlar
  - Pin Shield
  - Chipli kart dönüşümü
- ATM yüzeyinde delik açarak cash dispenser kablolarının dolandırıcının cihazına bağlanması ve komut gönderilmesi
  - Güçlü şifreleme
  - fiziksel doğrulama
- Network atakları
  - Personelin müdahalesi
  - Man in the middle atakları
  - Network cihazlarının ATM kabinin dışında olması
  - E-Mail ile zararlı yazılımın yayılması

# INTERNAL FRAUD

**EN BASİT AMA TRENDİ HİÇ KAYBOLMAYAN VAKALAR**

- İnaktif hesaplar
- Uzun vadeli mevduat hesapları
- Yaşlı müşteriler
- Yabancı müşteriler

# INTERNAL FRAUD

**ÖNEMLİ TRENDLER**

- Usulsüz krediler


- Zimmet > Müşteri / şirket zararı
- Satış Hedefleri / Zirvedeki personel
- Faiz oranı
- Teminat yapısı (Çek/senet/mevduat)
- Teminattaki çeklerin değişmesi

# INTERNAL FRAUD

**ÖNEMLİ TRENDLER**

- Masraf ve komisyonlar
- Rotatif krediler ve devre sonu faizleri
- Türev ürünler ve kompleks işlemler
  - Piyasa dalgalanmaları
  - Kâr/zarar dengesi
- Titan zincirleri
- Bilanço tahrifatları
- Doğrudan nakit paranın çalınması (sayım)

- Varlık özetleri/dökümleri ve hesap ekstreleri

- Telefon adres değişiklikleri

Mobil onay /SMS OTP

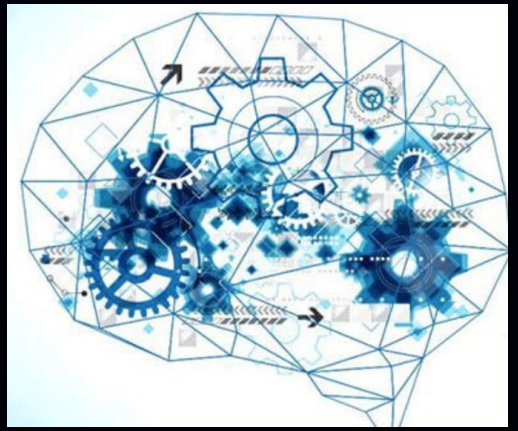
# INTERNAL FRAUD

**DOLANDIRICI DAVRANIŞLARI**

- İzne çıkmayan/ İzindeyken şirkete gelen personel
- Lüks yaşantı
- Yüksek borç / finansal zorluk
  - Kendisi
  - Ailesi

- Bahis / Kumar alışkanlıkları
- Riskli finansal ürünler
  - Türev piyasalar
  - Forex
  - Dijital Paralar (CryptoCurrency)
- Müşterek muhafaza – Görevlerin ayrılığı ilkesi
  - Anakasa
  - ATM
  - Çek/Senet

# NEDEN VERİ ANALİTİĞİ ?



**Geleneksel kural bazlı yaklaşımlar;**

- Hata oranı yüksek
- Zaman kaybı fazla
- Müşteri deneyimi kötü

**Veri Analitiği ve Makine Öğrenmesi**

- Hızlı ve isabetli karar
- Yüksek hacimli verilerden istatiksel anlamlı çıkarımlar
- Müşteri deneyiminde iyileşme

# MACHINE LEARNING NEDİR?

Genel prensip, fonksiyonun bulunmasıdır.

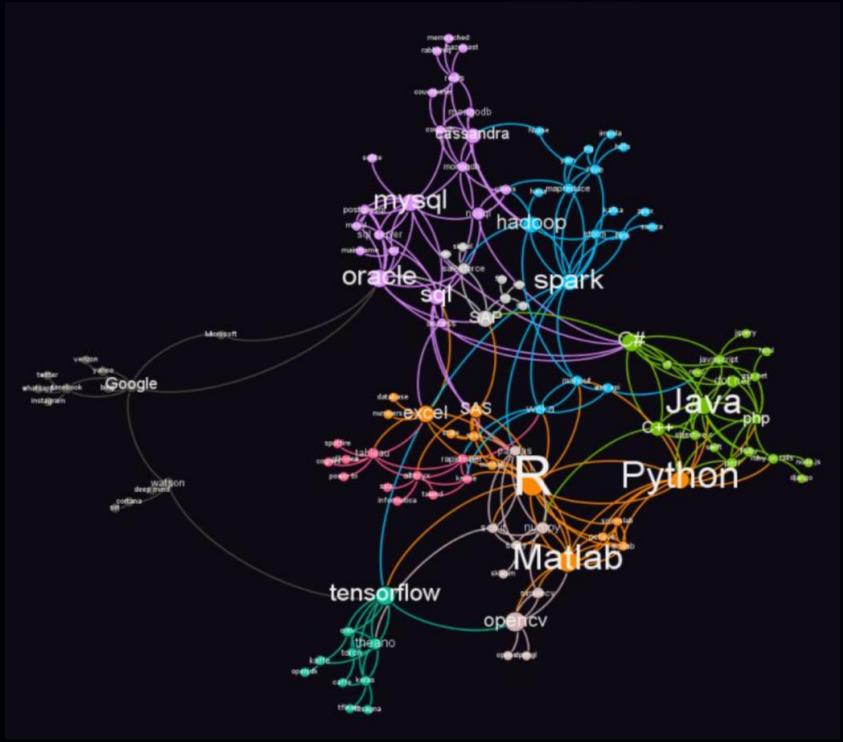
$$F(x) = y$$

# VERİ ANALİTİĞİ AŞAMALARI

İşin/Problemin mahiyetini anlama
Veriyi anlama
Veriyi uygun bir şekilde hazırlama
Modelleme
Değerlendirme
Devreye alma

# VERİ ANALİTİĞİ İÇİN KODLAMA DİLLERİ

1. Python
2. Java
3. R
4. C++
5. C
6. Scala
7. Julia



# VERİ HAZIRLIĞI

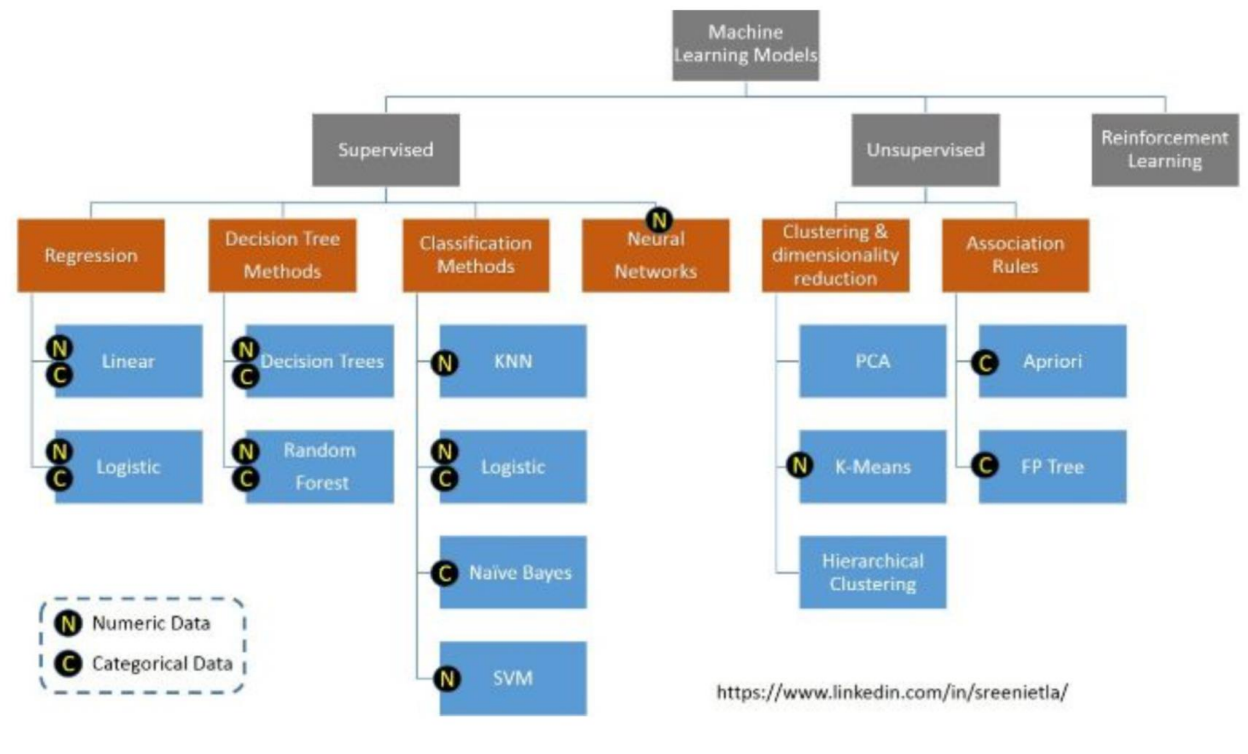
- Verinin uygun formlara dönüştürülmesi gerekir **(table, data.frame)**
- Eksik bilgilerin tamamlanması **(missing values)**
- Nümerik vs. Kategorik değişken ayrımı (iki yönlü geçiş mümkün)
- Normalizasyon (0 ile 1 arası)
- Kategorik değişkenlerin gruplanması

# MODELLEME

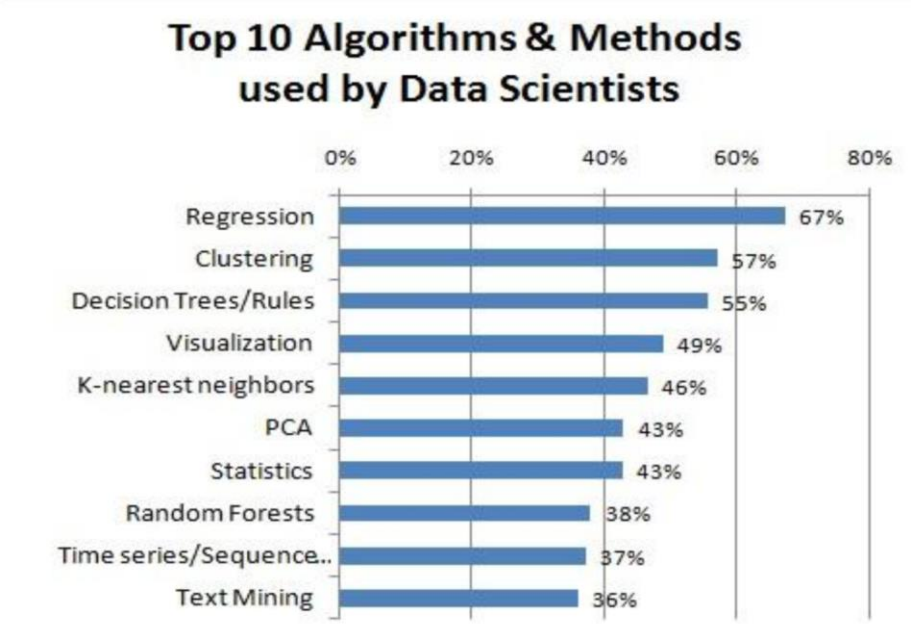
Supervised vs. Unsupervised Learning (Denetimli / Denetimsiz Öğrenme)

- Eğer etiketlenmiş veriler varsa (fraud/gerçek) denetimli öğrenme yapılabilir.
- Ancak etiketlenmiş bir değişken yoksa denetimsiz öğrenme uygulanır.

# MODELLEME


Machine Learning Models
Supervised
Unsupervised
Reinforcement Learning
Regression
Decision Tree Methods
Classification Methods
Neural Networks
Clustering & dimensionality reduction
Association Rules
Linear
Logistic
Decision Trees
Random Forest
KNN
Logistic
Naïve Bayes
SVM
PCA
K-Means
Hierarchical Clustering
Apriori
FP Tree
N Numeric Data
C Categorical Data
https://www.linkedin.com/in/sreenietla/

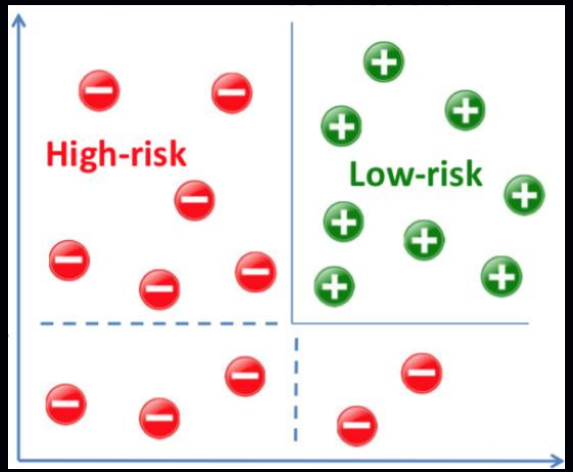
# MODELLEME


Top 10 Algorithms & Methods used by Data Scientists
0%
20%
40%
60%
80%
Regression
67%
Clustering
57%
Decision Trees/Rules
55%
Visualization
49%
K-nearest neighbors
46%
PCA
43%
Statistics
43%
Random Forests
38%
Time series/Sequence..
37%
Text Mining
36%

# MODELLEME

**Classification (Sınıflandırma)**

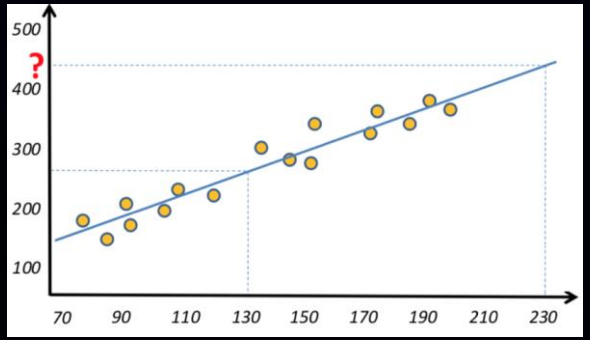
- Sınıflar kategoriktir. Bazı değişkenlerin birden fazla etikete sahip olabilir.
- Bir işlemin fraud olup olmadığı bir sınıflandırma problemidir.
- Bir işlemin fraud olma olasılığını ölçebilir.



# MODELLEME

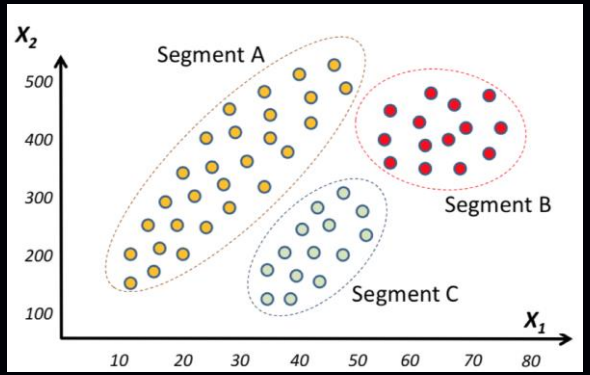
**Regression (Değer Tahmini)**

- Nümerik değişkenleri tahmin etme modelidir.
- Yaşanacak fraudun tutarını adedini tahminleyebilir.

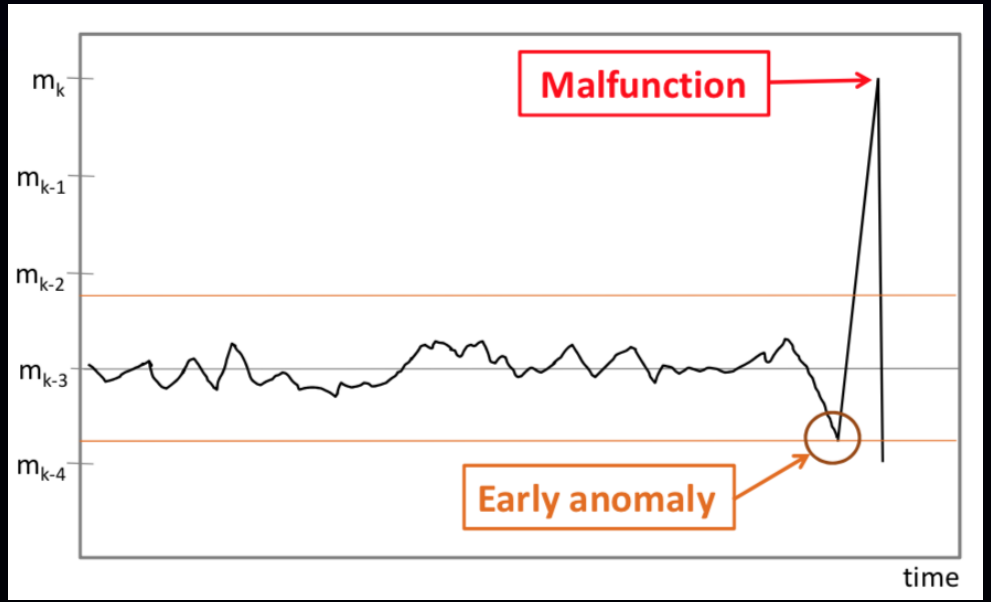



**Clustering (Kümeleme) -- Unsupervised**

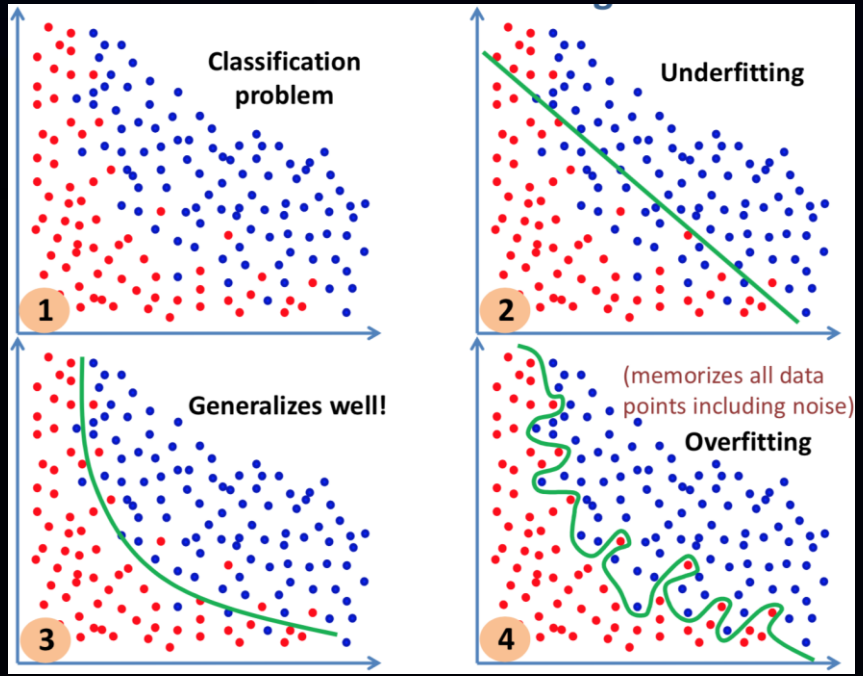
- Bir popülasyondaki öğeleri belirli özellikler çerçevesinde gruplara ayırmak/birleştirmek
- Otomatik Segmentasyon

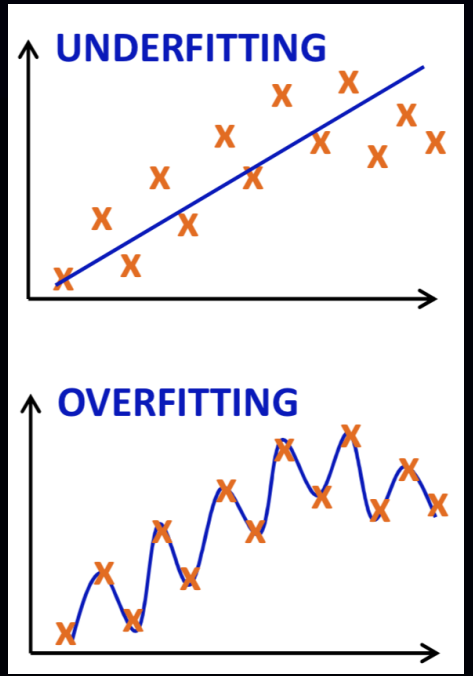


# ANOMALİ TESPİTİ



# GENELLEYEMEME RİSKİ




Bellek Funes adlı öyküde kusursuz hafızaya sahip Funes isimli bir genç vardır. İlk bakışta büyük bir talih gibi görünen ama aslında korkunç bir lanettir. Funes adlı kişi geçmişte herhangi bir zamanda gökyüzündeki bulutların şeklini tam olarak hatırlayabilir ama saat 3:15 te önden gördüğü bir köpeğin 3:14'te yandan gördüğü köpeğin aynısı olduğunu anlamakta güçlük çeker. Funes genelleme yapamaz.

# VERİNİN DENGESİZ DAĞILIMI

Kanser hastalığı/HIV virüsü gibi gerçekleşme ihtimali düşük olan veriler

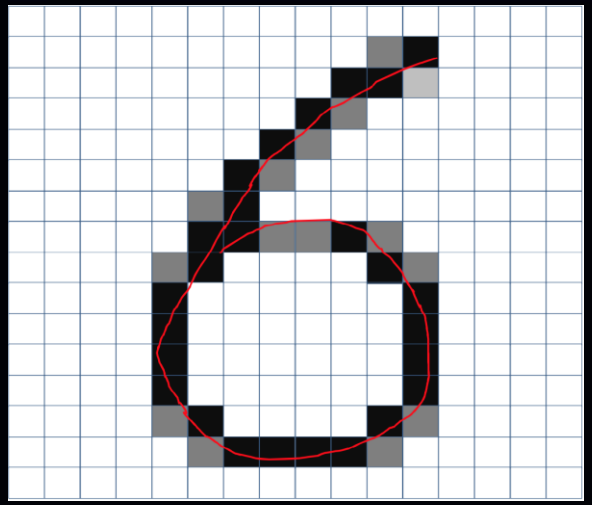
Fraud vakaları - % 1'in çok altında bir orana sahip.

Algoritma yaratmaksızın tüm işlemlere FRAUD DEĞİL etiketi verildiğinde dahi %99 başarı (accuracy) oranına erişilebiliyor.

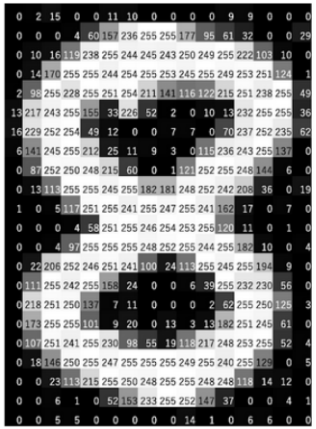
Ancak burada accuracy değil precision (kesinlik) devreye giriyor. Kanser hastasının veya fraudun tespit edilememesinin riski çok yüksek (false negative).

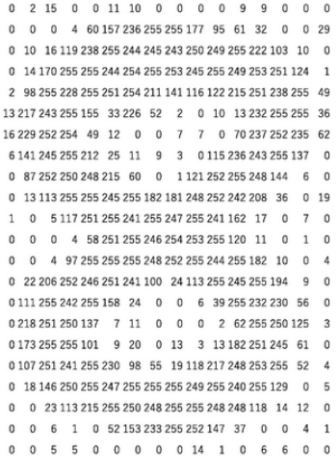
# RESİM İŞLEME

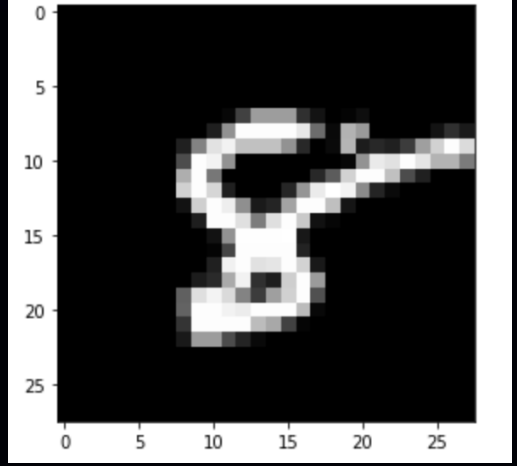
20x20bitmap:{0,1}400



# RESİM İŞLEME



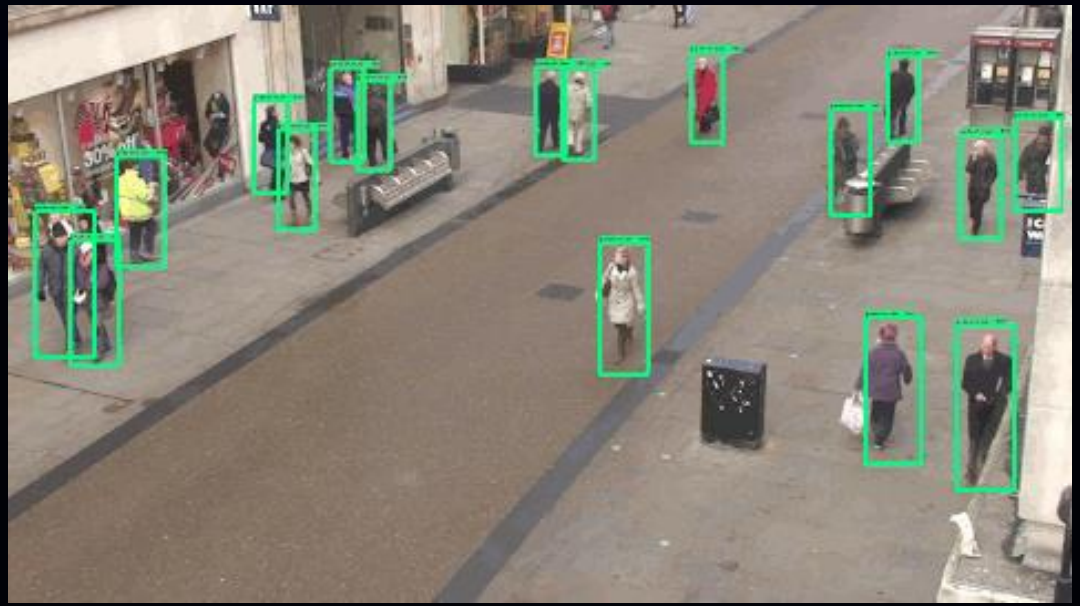





?

- İmza kontrolleri
- İmzanın konumu

# VIDEO İŞLEME



Giriş çıkış kontrolleri

# TEŞEKKÜRLER

FEATURE SPACE

OUTSMART RISK

# Fraud Monitoring in Retail Banking and Issuing

Mark Taylor

# Introduction

OUTSMART RISK

- Joined Featurespace in May 2019 as a Fraud Market Expert, focussing on Financial Services.
- I have worked in the fraud & risk industry for over 18 years.
- Prior to joining Featurespace, I worked at Metro Bank, Barclays & RBS, where I was responsible for Card & Digital Fraud.

# Remote Banking Payment Fraud

OUTSMART RISK

## Online

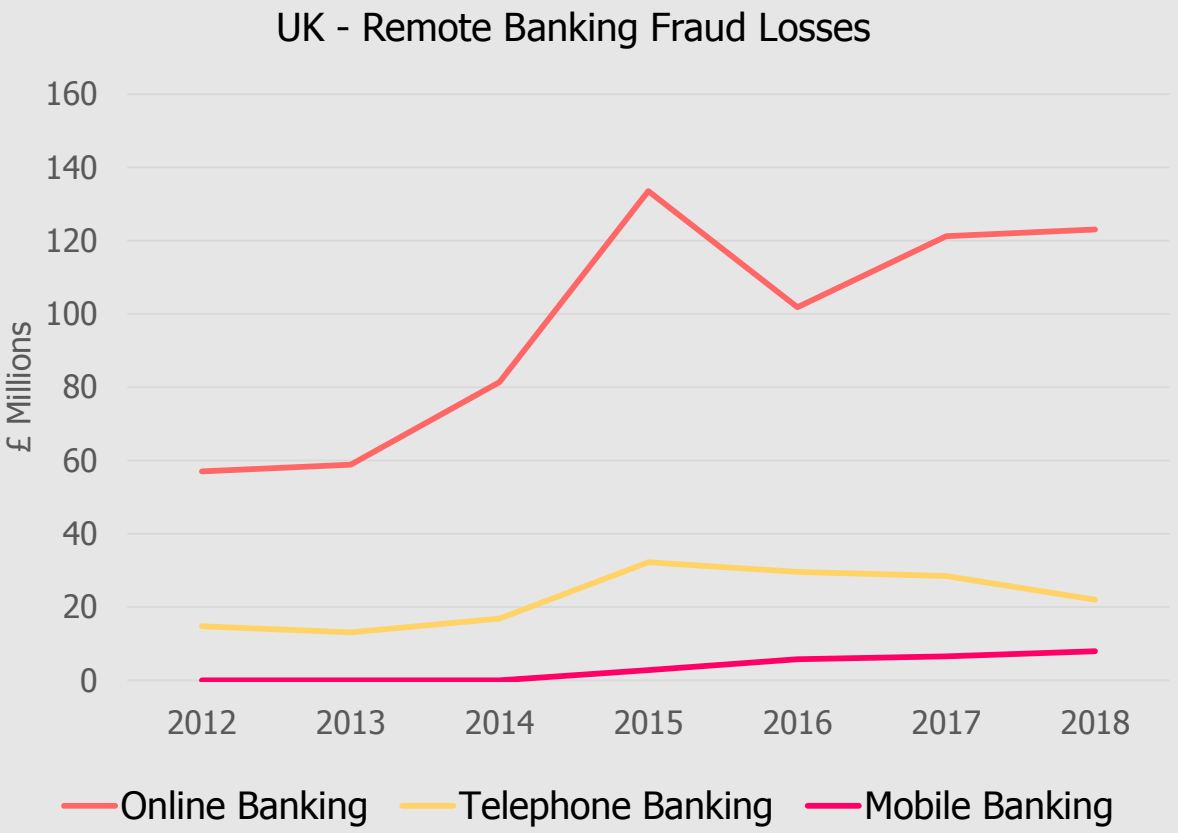
- £123m
- +1% YoY

## Mobile

- £7.9m
- +20% YoY

## Telephone

- £22m
- -22% YoY



# Social Engineering

OUTSMART RISK

Vishing

Phishing

Smishing

# Account Takeover Fraud: The multi-channel attack

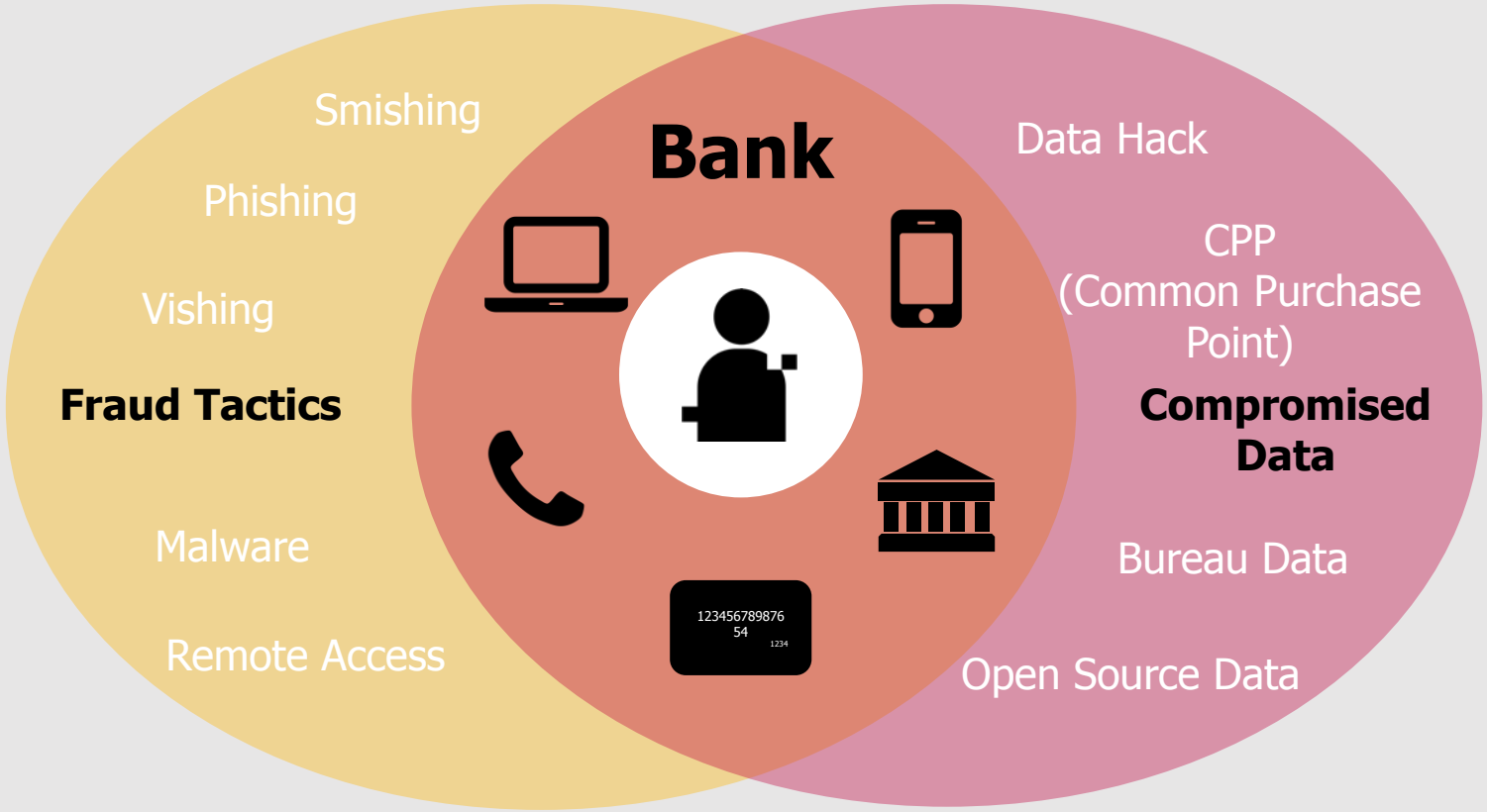
OUTSMART RISK

1. **Fraudster starts with basic data** (Social Engineering or Compromised Data)

2. **Data can be enriched** (Further Social Engineering or by obtaining credit reports)

3. **Fraudster targets weaknesses within banking channels** (Passing ID&V or Online Banking using credentials obtained from Social Engineering)

4. **Fraudster takes Control of Customer Account** (funds withdrawn, can include lending)



# Remote Access Trojans (RAT)

OUTSMART RISK

1. Phishing email containing malicious file

2. Compromising user credentials and download remote access tool

3. Fraudster calls customer

4. Customer accessing online banking

5. Fraudster takes over online banking session

6. Fraudster transfers customers funds

# Authorized Push Payment Scams

OUTSMART RISK

## What are Authorized Push Payment Scams?

In an Authorized Push Payment Scam, a fraudster manipulates their victim into sending money directly from their account to an account which the criminal controls, often using social engineering tactics such as phishing, vishing or smishing to gain the victims trust.

### Purchase scam

The victim is scammed into paying for goods that they never receive.

### Investment scam

The victim is scammed into investing money in a fake investment, such as property or land.

### Romance scam

The victim is scammed into paying funds to a person they have met through online dating sites. Fraudsters create fake profiles to build a relationship with the victim.

### Advance fee scam

The victim is scammed into making a payment for a fee which will release a higher value payment, for example, an overseas lottery.

### Invoice & Mandate scam

The victim attempts to pay a legitimate payee but the fraudster intervenes to trick the victim into sending funds to an account they control. Often the fraudster will have access to the victim's email account so they can pose as a known 3rd party.


### CEO Fraud

The fraudsters impersonate a CEO of a company and requests the victim to make a payment to an account they control. Finance teams are often targeted with these types of scams.

### Impersonation/imposter

The fraudster poses as someone else - often police, bank or government staff - and requests the victim send money to an account they control. The fraudster will often tell the victim that they or their account is at risk.

# Authorized Push Payments Scams

OUTSMART RISK

## Impact of faster payment

Countries which have implemented faster payments are particularly vulnerable to Authorized Push Payment scams, as proceeds can be cashed out before the victim or their bank is aware of the scam.

Where other markets are moving towards providing faster payments, consumer groups are reporting an increase in scam activity.

**93%**

Of UK scam payments were made using Faster Payments

**£354m**

Customer reported scam losses in UK in 2018

**$488m**

Customer reported scam losses in US in 2018

**$107m**

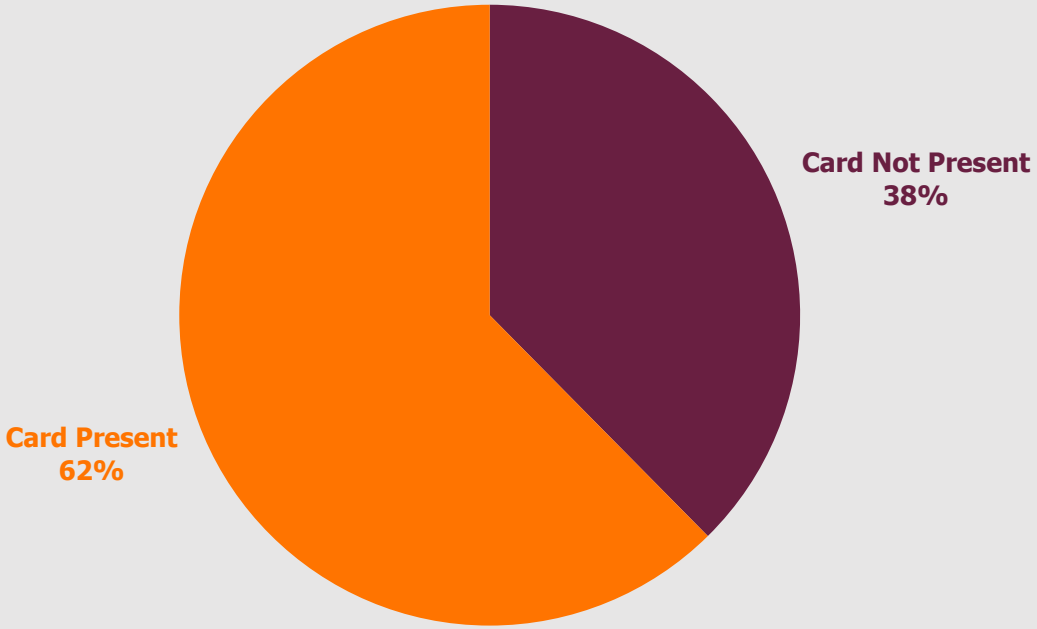
Customer reported scam loses in Australia in 2018

| | 2017 | | | 2018 | | |
|---|---|---|---|---|---|---|
| | Personal | Business | Total | Personal | Business | Total |
| Victims | 38,596 | 5,279 | 43,875 | 78,215 | 6,409 | 84,624 |
| Value (£M) | 107.5 | 128.6 | 236.1 | 228.4 | 126 | 354.3 |
| Recoveries (£M) | 22.6 | 38.2 | 60.8 | 42.3 | 40.3 | 82.6 |

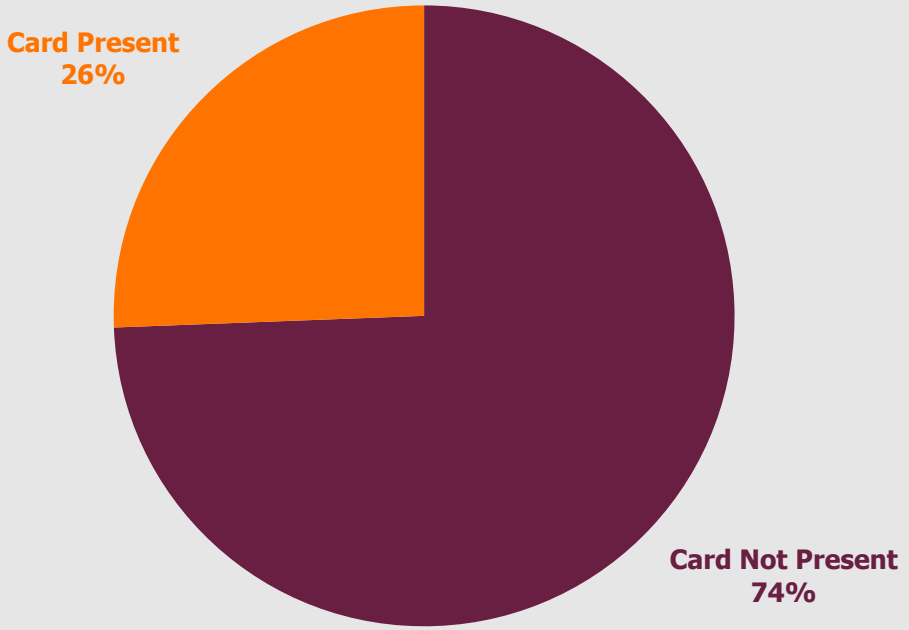
# Where is all the card fraud

OUTSMART RISK

## GLOBAL TOTAL APPROVED TRANSACTİON VOLUME SPLİT




## GLOBAL FRAUD TRANSACTİON VOLUME SPLİT




**74%** of card frauds sits within **38%** of all card activity

# Fraud as a Service: Enabling the opportunistic fraudster

OUTSMART RISK

- ✓ **$30 Average cost for card data with CVV, DOB**
- ✓ **$550 Cloned card with $10,000 balance**
- ✓ **$1200 Card skimmers**

- ✓ **$40 Full customer data**
- ✓ **$1,500 Bank credentials for Top UK banks with balance $20k**
- ✓ **50,000 Spam emails $60**

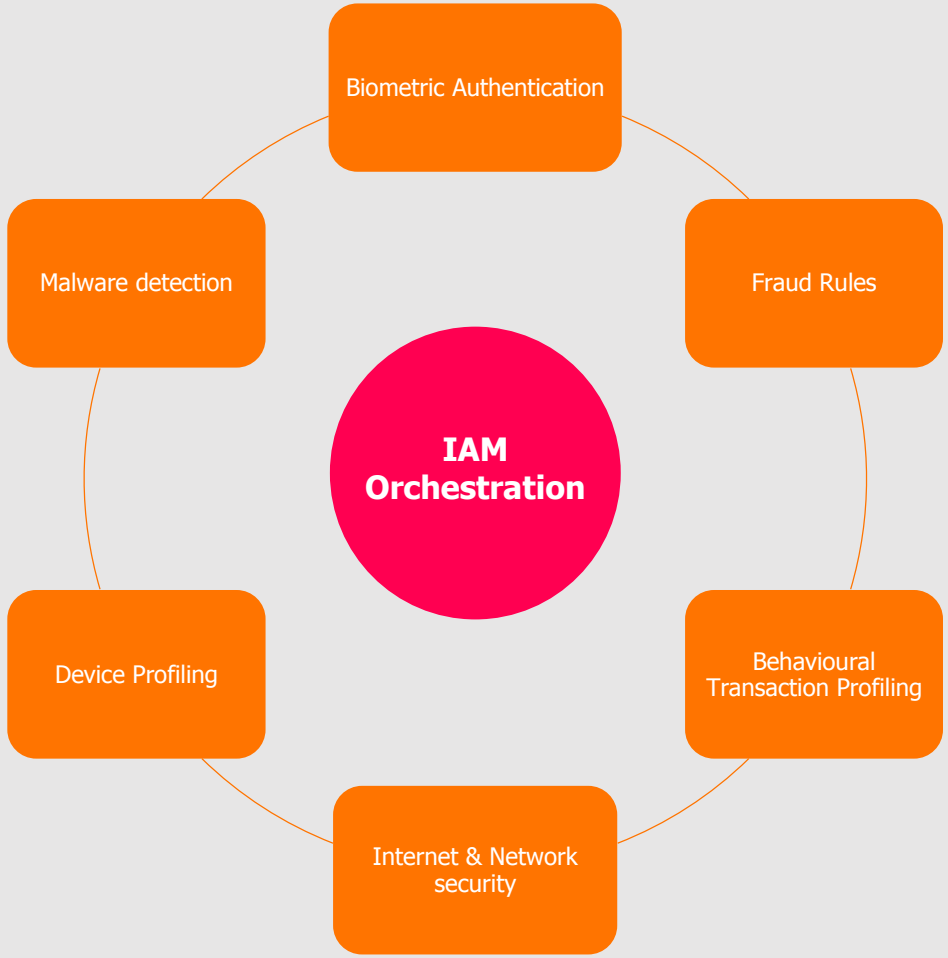
# Multiple layers of security

OUTSMART RISK

By implementing many different layers of security, your organization can respond to emerging fraud threats that may otherwise overcome a standalone solution.

Orchestration of fraud scores will ensure optimum results for low false positives and increased fraud detection.

Organisations can adjust controls in real time to close down threats and implement new strategies



# Looking into 2020

OUTSMART RISK

## PSD2 – SCA:

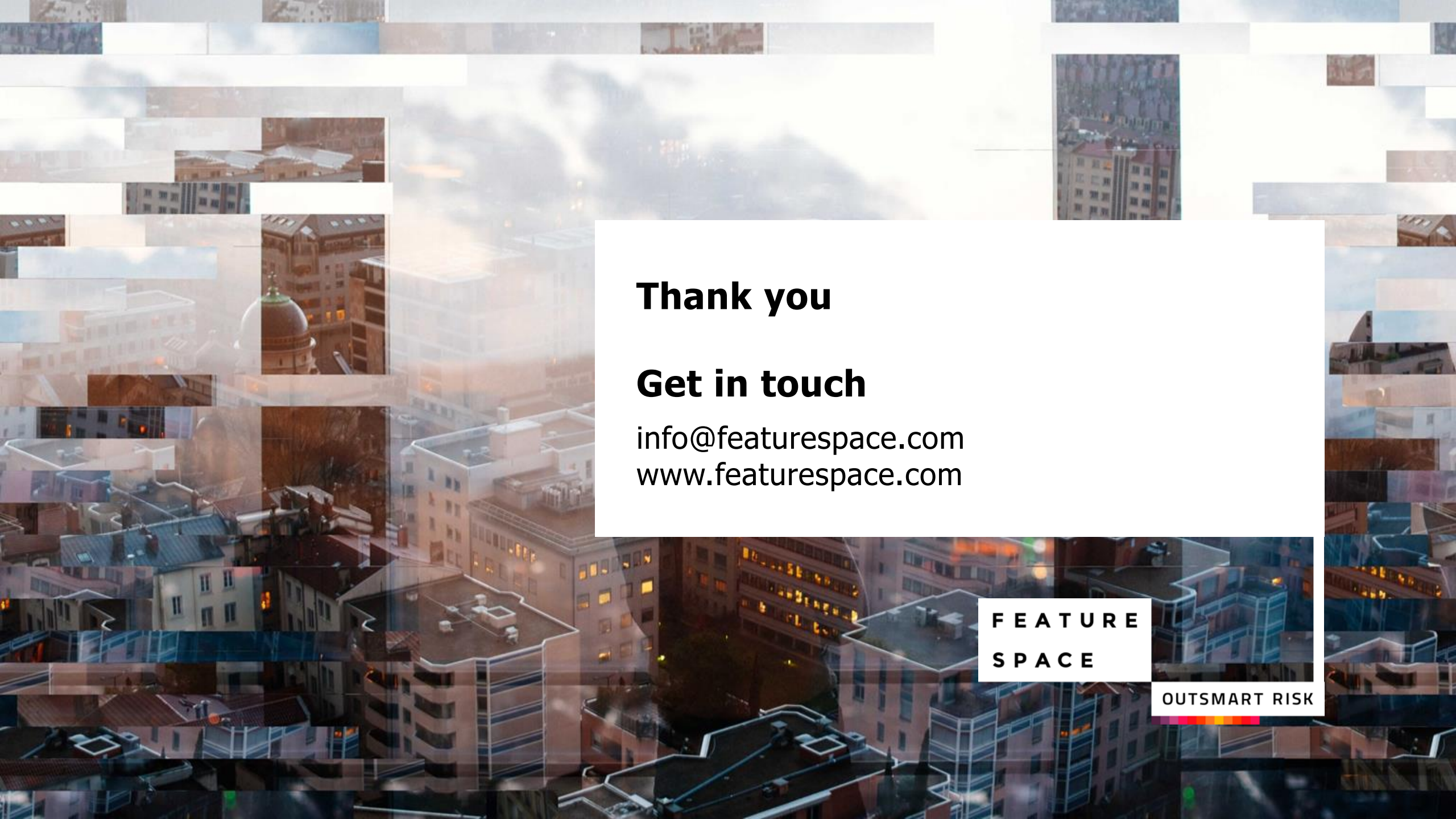
- Stronger Customer Authentication – Global adoption (Cards & Online Payments)
- Increased merchants going 3DS (liability shift to Issuers)
- More countries utilise 'Open Banking' API's
- New TPP's

## Faster Payments:

- More countries moving to faster payments
- Reduction in fraud recoveries

## PSR – Contingent Reimbursement Model:

- More regulation around APP scam victims
- Potential further liability shift to the banks



## Thank you

## Get in touch

info@featurespace.com
www.featurespace.com

FEATURE SPACE

OUTSMART RISK

FEATURE SPACE

OUTSMART RISK

ACFE

Association of Certified Fraud Examiners

# Fraud Monitoring in Acquiring

**Roger Lester – SME, Featurespace**

Thursday 21st October, 2019

# Introduction – Who am I?

OUTSMART RISK

- Joined Featurespace in 2015 as a Subject Matter Expert, focussing in Financial Service, specifically payments.
- I have been in the card Industry for over 30 years.
- Prior to joining Featurespace I worked at First Data and Lloyds Bank both as an Issuer and an Acquirer.

FEATURE SPACE

# Worldwide Fraud Trends

OUTSMART RISK

| | Q4 2016 | Q3 2018 | Q4 2018 |
|---|---|---|---|
| Gross Fraud BPs | 100 | 88 | 90.6 |
| Net Fraud BPs Acquirer | 52.7 | 48.8 | 50.2 |
| Net Fraud BPs Issuer | 47.3 | 39.2 | 40.4 |

FEATURE SPACE

# Regional Fraud Trends

OUTSMART RISK

| | Q1 2017 | Q4 2018 |
|---|---|---|
| U.S. | 80.6 | 63.2 |
| Canada | 45.4 | 37.2 |
| Latin/Caribbean | 33.8 | 26.7 |
| Asia/Pacific | 26.9 | 19.7 |
| Middle East/Africa | 20.8 | 13.1 |
| Europe | 10.2 | 10.1 |

FEATURE SPACE

# Regional Fraud Trends

OUTSMART RISK

## Card Not Present – Gross Merchant Fraud BPs

| | Q4 2016 | Q3 2018 |
|---|---|---|
| Latin/Caribbean | 461.9 | 399.4 |
| Middle East/Africa | 308.8 | 230.9 |
| Europe | 226.4 | 203.5 |
| U.S. | 172.9 | 152.0 |
| Canada | 165.6 | 156.4 |
| Asia Pacific | 161.7 | 180.8 |

FEATURE SPACE

# Challenges/Trends for 2020

OUTSMART RISK

- CNP continues to grow
- Risk and reward continues to be a balancing act
- Combining Issuing and Acquiring data
- Consumer reaction to Stronger Customer Authentication (SCA)
- Social Engineering
- Refund fraud
- Real time fraud monitoring will be key
- Behavioral analytics and machine learning

FEATURE SPACE

# Thoughts to Takeaway

OUTSMART RISK

- Do not rely on rules alone
- Collaboration
- 3Ds 2.0+
- Consider controls to mitigate Account Takeover and First Party fraud

FEATURE SPACE


FEATURE
SPACE
OUTSMART RISK