

Run-time transaction scoring for payment fraud prevention



Nikolaus D. Bayer | 26 September 2016 | COST Action IC1402

Run-time transaction scoring for payment fraud prevention



Nikolaus D. Bayer | 26 September 2016 | COST Action IC1402

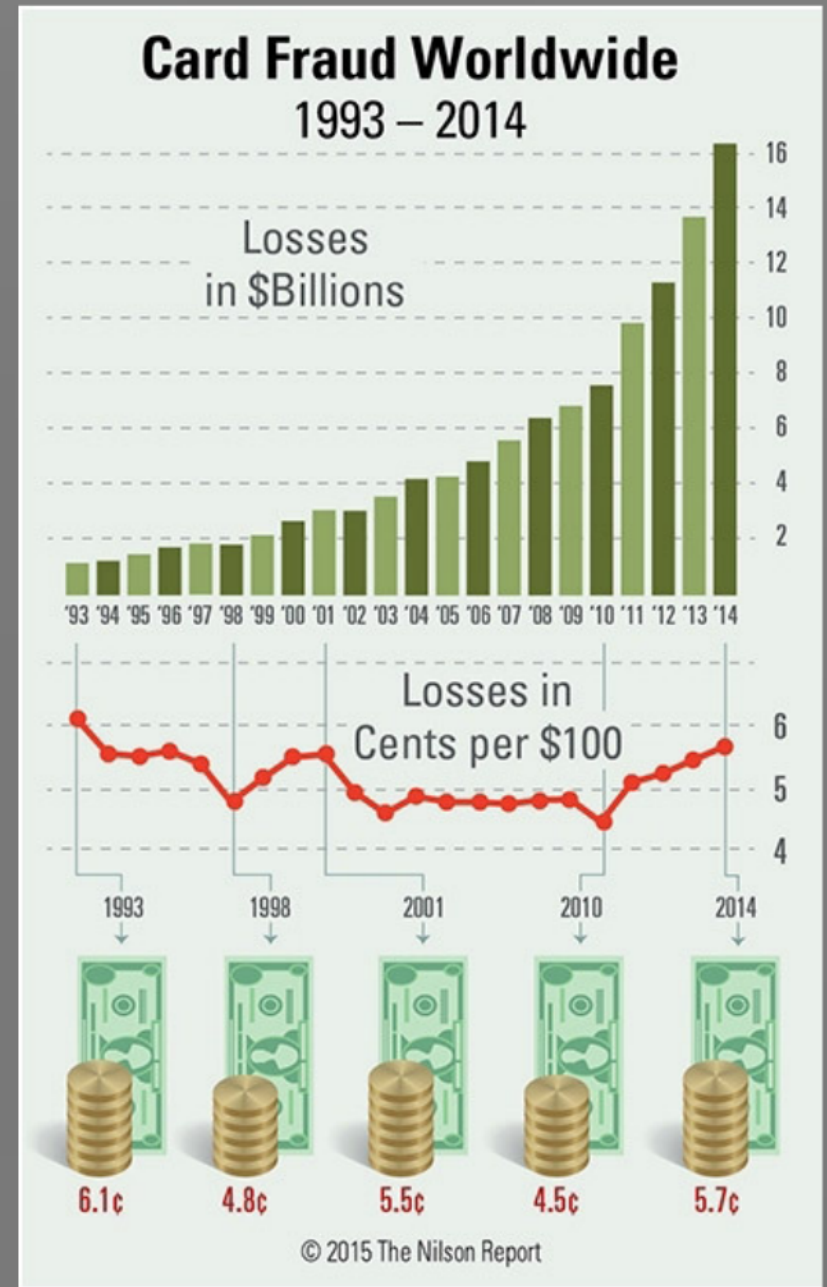
Hi! - About me

- Born 1976 in Osnabrück, Germany
- Studied Computer Science in Aachen and Madrid
 - Artificial Intelligence, Operations Research
- Learned about card payments and fraud at First Data Corp.
- Co-founded IRIS Analytics GmbH in 2007
 - Risk and fraud management in electronic payments
 - Exit to IBM by end of 2015

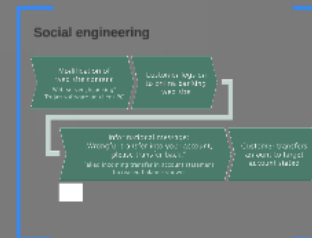
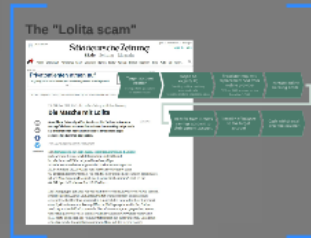


What are talking about?

- **Organized crime** drives payment fraud.
- **"PayPal is a risk management** company with an attached payment function."
- **Huge data volumes**
 - EU: 47bn card payments in 2014
 - France: 750tps peak
 - < 50ms for fraud scoring



Some real life examples



"Clean fraud"

- All transactions are **technically** and **formally valid**.
- We thus need to **monitor** payment channels for "**abnormal**" behaviour.

Counterfeit credit card

2

1



The "Lolita scam"

München 14°

Süddeutsche Zeitung
SZ.de Zeitung Magazin

Jobs Immobilien Anzeigen
Login Abo

Politik Wirtschaft Panorama Sport München Bayern Kultur Wissen Digital Chancen Reise Auto Stil mehr...

ANZEIGE

Privatpatienten atmen auf

Langjährig Versicherte können jetzt den Beitrag senken. Allerdings-mehr

Home > Digital > Betrug beim Online-Banking mit mTan: Masche mit Lolita

29. Oktober 2013, 11:49 Uhr mTan-Betrug im Online-Banking

Die Masche mit Lolita

Ausspähen, Daten abgreifen, kassieren: Die Zahl der bekannten Betrugsfälle beim mTan-Verfahren im Online-Banking steigt. Nach SZ-Informationen haben Kriminelle bei Bankkunden sogar sechsstelligen Summen abgehoben.

Von Harald Freiburger, Frankfurt

Feedback

Die Betrugsserie mit dem mTan-Verfahren im Online-Banking zieht weitere Kreise. Nach Informationen der SZ sind inzwischen zwei Fälle mit jeweils sechsstelliger Schadenssumme bekannt geworden. So hoben Betrüger am 20. September 182.000 Euro vom Postbank-Girokonto eines 60-jährigen Hamburgers ab. "Es handelt sich um meine gesamten Ersparnisse, ich weiß bis heute nicht, ob ich das Geld zurückbekomme", sagt er. Ein 44-Jähriger in Emden verlor 125.000 Euro.

Die Täter gingen genauso vor wie bei mindestens neun weiteren Fällen, die sich zwischen Mitte August und Anfang Oktober im gesamten Bundesgebiet ereigneten. Die Betrüger spionierten zunächst den Computer ihrer Opfer mit einer Spähsoftware aus. Dann griffen sie die Zugangsdaten für das Online-Banking und Mobilfunk-Daten ab, die auf dem Computer gespeichert waren. Gleichzeitig bestellten sie beim Mobilfunk-Anbieter des Opfers eine zweite SIM-Karte und ließen die Nummer telefonisch auf diese umleiten. Daraufhin erhielten sie die Transaktionsnummern (Tan) auf das eigene Handy.

Target account creation

Using a fake passport or identity card

Trojan on victim's PC

Stealing online banking access details
Stealing mobile telephone data

Fraudster requests replacement SIM from mobile provider

OTP via SMS are sent to the fraudster's SIM

Increase online banking limits

Transfer from victim's savings account to their current account

Transfer of balance to the target account

Cash withdrawal (over the counter)



Target account creation

Using a fake passport or identity card

Trojan on victim's PC

Stealing online banking access details
Stealing mobile telephone data

Fraudster requests replacement SIM from mobile provider

OTP via SMS are sent to the fraudster's SIM

Increase online banking limits

Transfer from victim's savings account to their current account

Transfer of balance to the target account

Cash withdrawal (over the counter)

Banking

bekannten
g steigt. Nach
sogar

ANZEIGE

Online-Banking
sind

etrüger am
konto eines
meine gesamten Ersparnisse,
ekomme", sagt er. Ein



▼ Online-Banking

 Abmelden

[direkt zu:](#)

- Bitte auswählen -

[Startseite](#)

Finanzstatus

Kontodetails

Umsätze

Banking

► Privatkunden

Finanzstatus

 Nach Kontoinhabern sortieren Giro-Detail-Übersicht

Sehr geehrter Kunde,

aufgrund der SEPA-Umstellung ist eine Fehlüberweisung auf Ihr Konto 16000000000000000000 verbucht worden. Die Struktur des Sicherheitssystems von unserem Onlinebanking lässt nur Zahlungen mit Ihrer Freigabe zu. Damit Sie Ihr Konto weiterhin wie gewohnt nutzen können, muss die Rückzahlung der Fehlüberweisung von Ihnen freigegeben werden.

Ihr Guthaben, alle weiteren Unterkonten und Sparguthaben sind davon nicht betroffen. Es entstehen keine Transaktionskosten oder andere Nachteile für Sie. Bis zur Rückzahlung können Sie Ihr Konto nicht benutzen. Falls Sie keine online Rückzahlung tätigen, erhalten Sie in den nächsten Tagen einen Brief, mit dem Sie zu Ihrer Filiale gehen müssen, um die Überweisung auszuführen.

Bitte erledigen Sie dies umgehend um Ihren Zugang sofort wieder frei zu schalten.

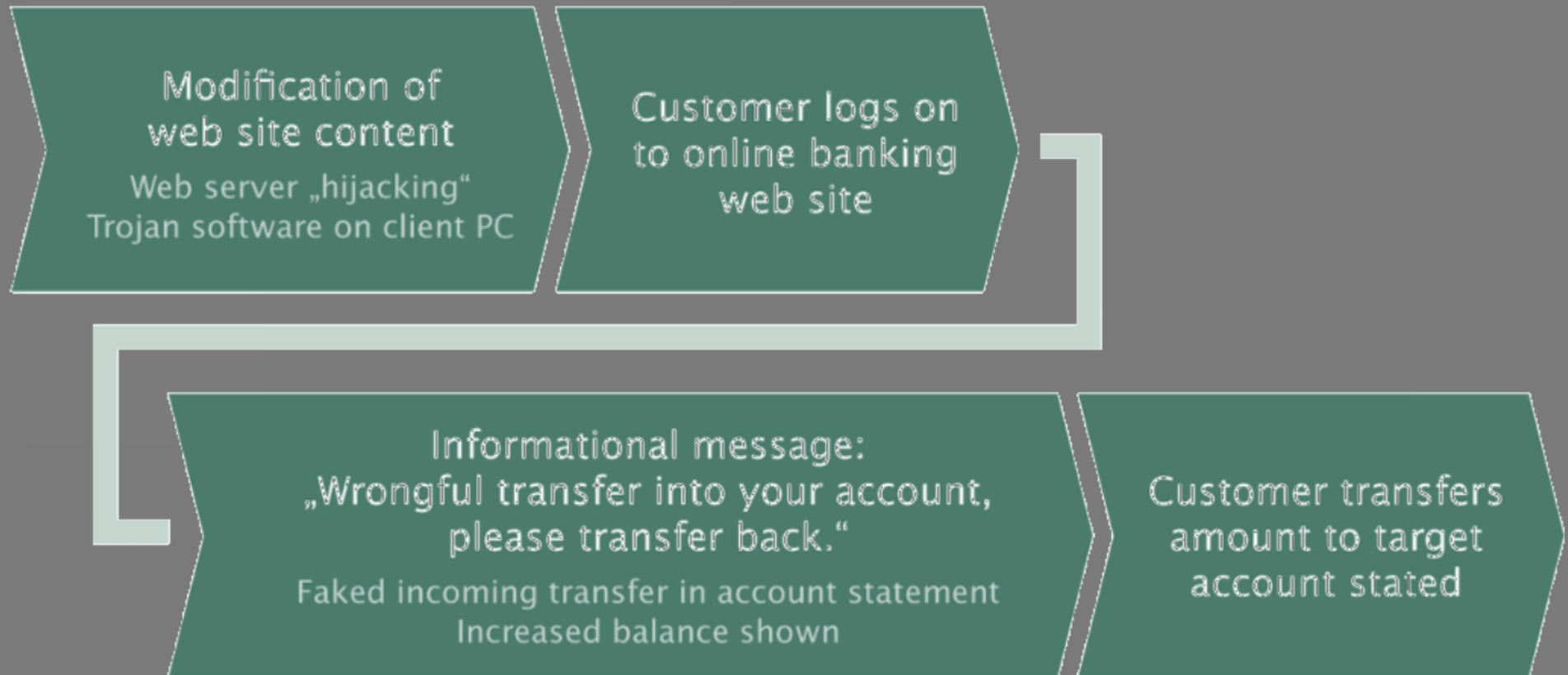
Informationen der Fehlgutschrift:

Auftraggeber	Finanzamt
IBAN	DE44 2512 0510 0007 0001 0001 00
BIC	2512031
Betrag	7.700,00 EUR
Verwendungszweck	Steuererstattung 2015

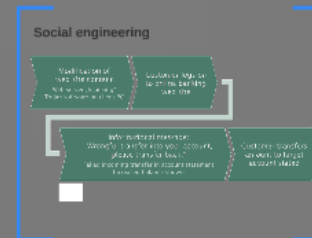
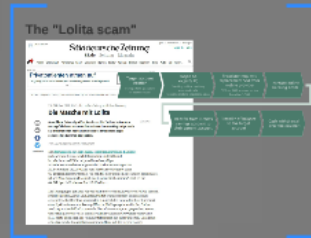
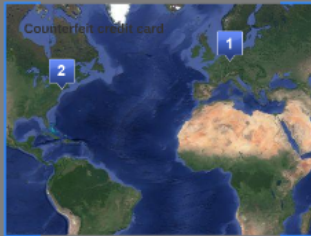
Kontoauszug anzeigen

Rückbuchung durchführen

Social engineering



Some real life examples



"Clean fraud"

- All transactions are **technically** and **formally valid**.
- We thus need to **monitor** payment channels for "**abnormal**" behaviour.

Main challenges

Class overlap

Fraudsters adapt genuine behaviour

Skewed class distribution

99.7%
vs
0.3%

Frequent model changes

3+ times per week

Need sandbox testing

Huge data volume

100bn+ payments p.a. in EU

1000+ tps peak

Curse of dimensionality

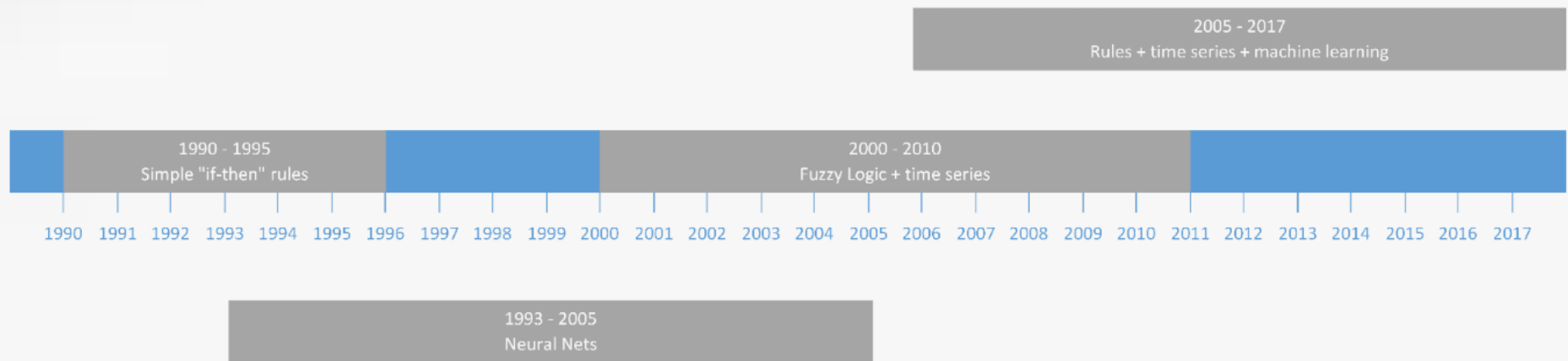
100+ data attributes

Time series evaluation

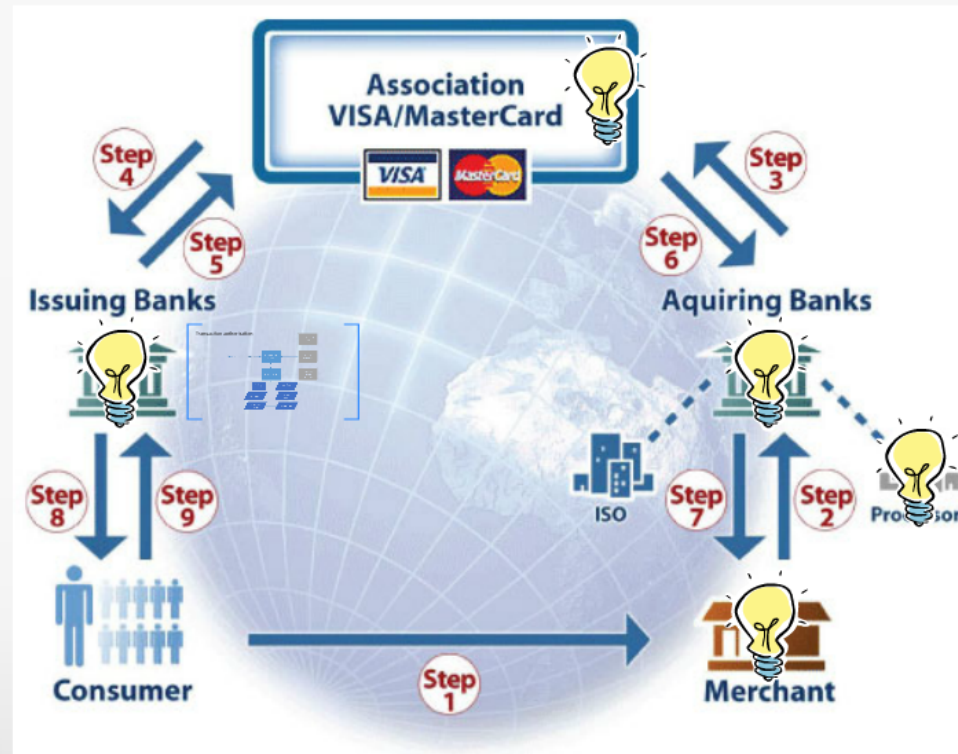
Real-time operation

< 5ms response time

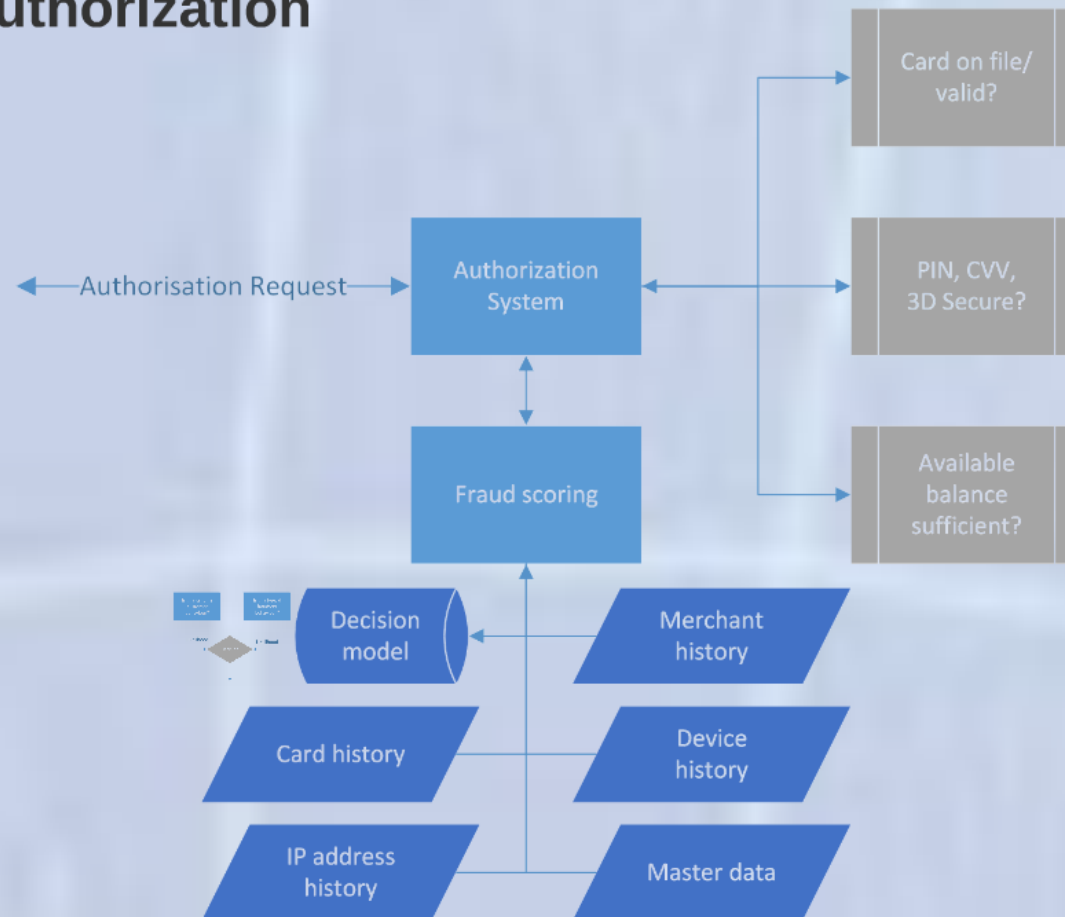
A large bouquet of Artificial Intelligence...

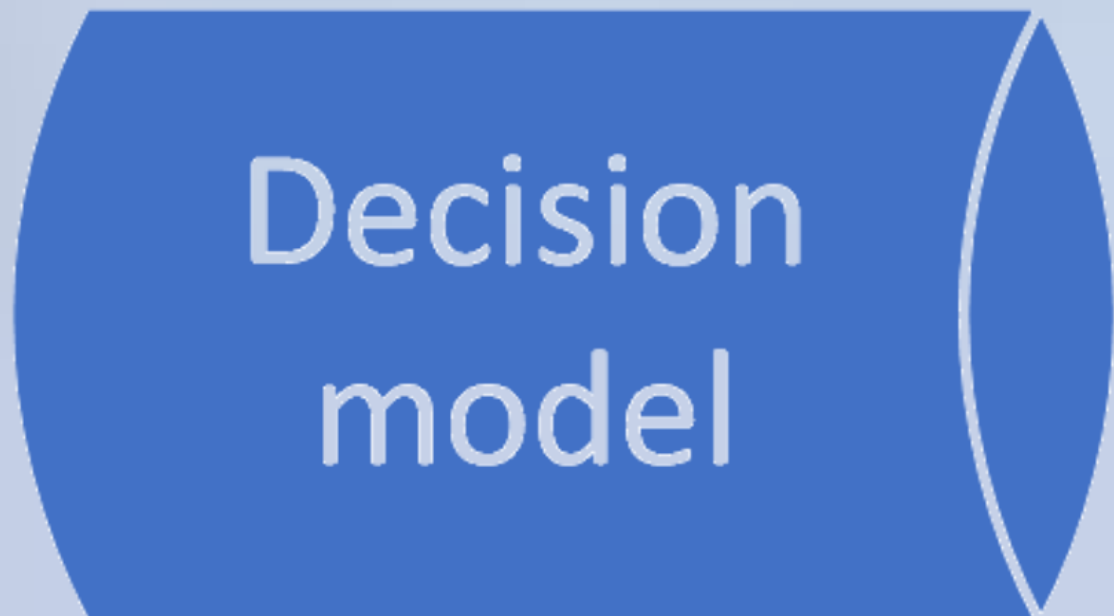
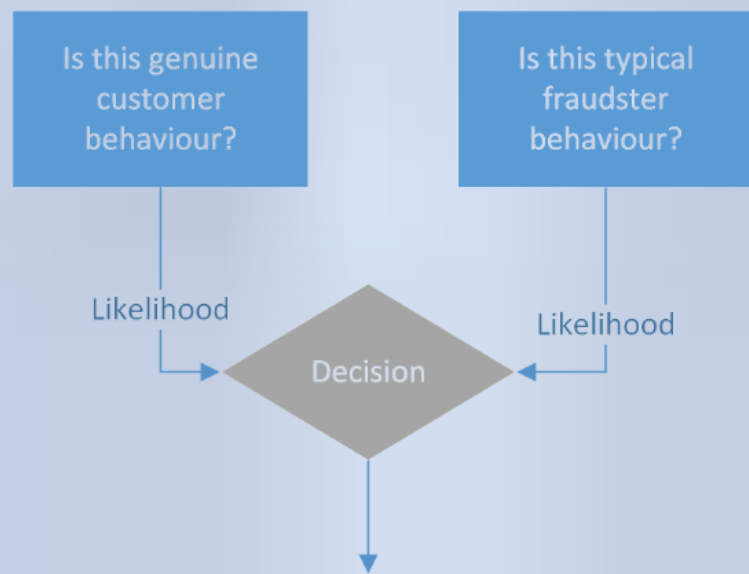


Transaction flow



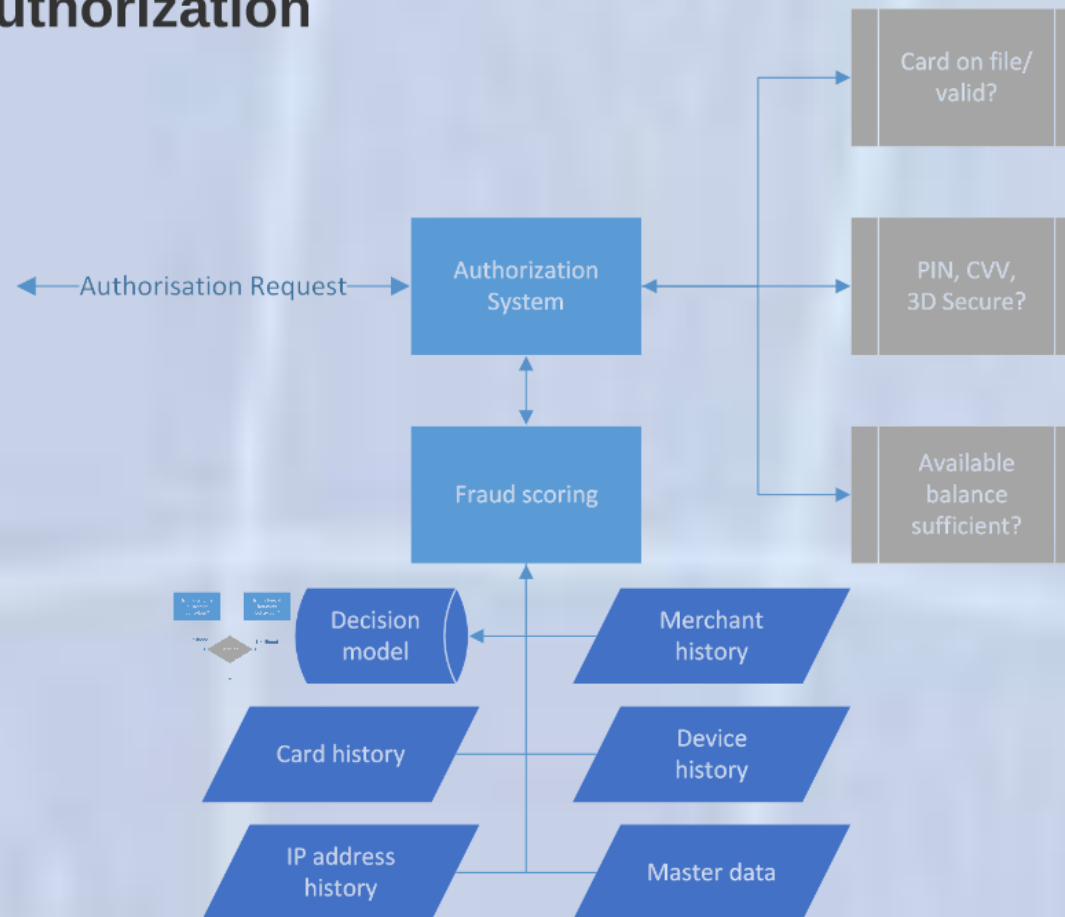
Transaction authorization



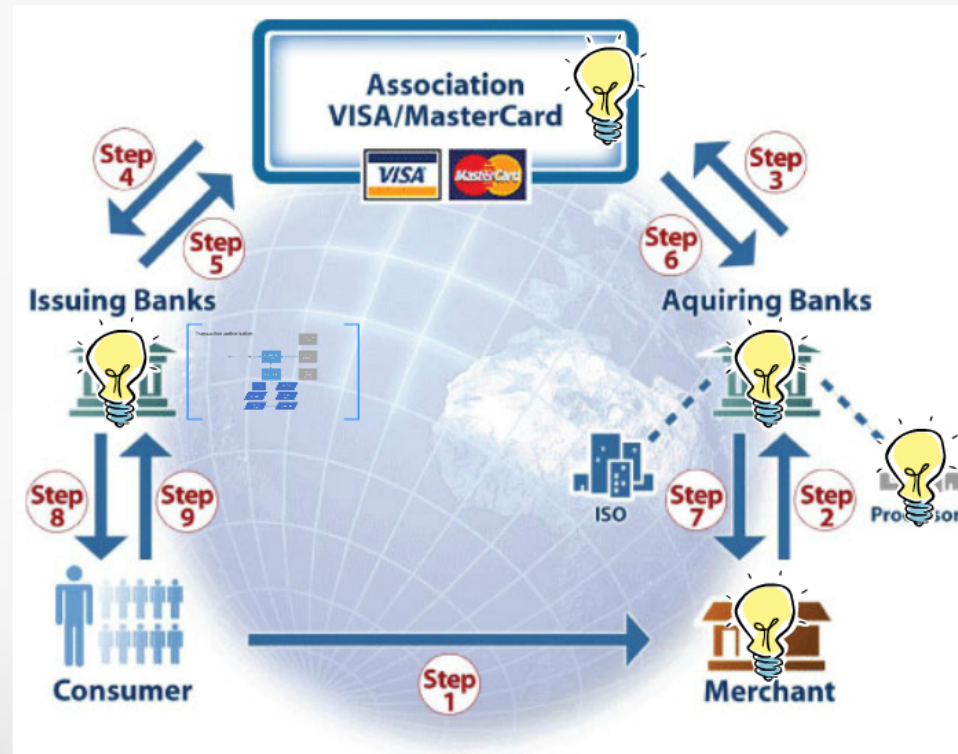


Card history

Transaction authorization



Transaction flow





So much for today - of course there is much more

- **Compliance**, regulatory topics
- Data **security**
- **High availability**, 24/7 operations
- Operations **workflows**
- Defining the **right target function**
- ...

Nikolaus D. Bayer
nikolaus.bayer@gmail.com
+49 170 5733 702

<https://de.linkedin.com/in/nikolausbayer>