mobey forum
mobile financial services

Security and compliance: from a showstopper to an advantage

Leader: Martin Wimmer, Erste Group

Vienna
11 December, 2014

Challenges

- EU Regulation – MIF, PSD2 (esp. Account info, payment initiation)
  - How will third party providers act on „our“ infrastructure with regard to authentication, security, ris,
- PCI DSS, standards, certifications
- Card schemes regulations
- Future of authentication („strong authentication“, biometrics, tokens…)
- Mobile (payments) security
  - Secure Elements (SIM centric, eSE, Cloud…)
  - Tokenization
  - remote vs. proximity – convergence of payments
  - Handset security
  - …
- Financial inclusion
- Data protection issues
- …

How to overcome the threats / Ideas to make threats to opportunities

- Regulation will probably lead to more electronic payments – how can we benefit?
- Cross selling opportunities (includes mobile marketing/selling via beacon technology)?
- Big data opportunities?
- Extend our scope and card usage – e.g. with transit applications (via paywaye &/or paypass)
- Future of online credit transfers? European wide..
- Financial inclusion opportunities (e.g. prepaid, other banking products)?
- Own European wide card scheme Co-badged with a int. Scheme for usage abroad

The most thought-provoking/ surprising / “ahaa-” idea

- A bank can become a Third party provider using the PSD2 „opportunity“ to get account info and initiate payments from other bank competitors
  - But under a neutral name and not the bank name. E.g. PayPal is seen by the customers as neutral company, which is their brand core/positioning
- Own European wide card scheme Co-badged with a int. Scheme for usage abroad

Summary I

- Banking = TRUST and this is a main difference to Facebook, Google and others so we need to act more solid and serious with all pros and cons
  - Data protection
  - Regulation etc.
- PSD2 - (esp. Account info, payment initiation)
  - How will third party providers act on and with „our“ infrastructure with regard to authentication, security, risk etc. – unknown
- Convenience and user experience are key for the user (see PayPal respectively other User Name & PW-solutions or Touch ID from Apple BUT will it continue with PSD2) – maybe yes, when somebody (the bank) takes the risk

Summary II

- Future Authentication methods (e.g. 2 factor like PW and Card reader or Biometrics) depends on the Risk Management resp. Limit Management and can be seen as competitive advantage between banks
- Authentication methods have to be fast & mobile (e.g. Card readers are not perfect for the mobile world but ok for the desktop PC but world goes mobile)
- Embedded SE (using TEE) can also be used to make the phn more secure for authentication also and not „only“ for payments
- Cross selling of bank products in netbanking and mobile banking apps – we should use bank data much more as we do it today (our DATA and not BIG DATA)

Summary III

- Mobile Marketing – cooperation models between the bank with partners to enter the mobile marketing area (can bring additional revenues for the bank)
  - Example netbanking: we have logos from retailers etc. e.g. in George – we could integrate partner apps in netbanking/George and negotiate with the main merchants for a reward structure for our clients or a supermarket to enable time saving pre-packaging etcetc.

NETBANKING can be a „MARKETPLACE“/PORTAL TO PARTNER APPS/WEBSITES

THE MORE CONNECTED THE CLIENT IS WITH THE BANK AND OUR PARTNERS THE LOWER IS THE PROBABILITY THAT THE CLIENT LEAVES OUR BANK (= CUSTOMER RETENTION)

Summary IV

- Can we use the customer data? Not everywhere because of legal stuff but we can get the customer approval to use their data when we can promiss the 2 most relevant benefits which are
  - TIME SAVING for the client &
  - MONEY (reward, bonus, cash back, merchant coalition)