Combating fraud and money laundering

Hans Lindberg

May 2024

Svenska
Bankföreningen
Swedish Bankers' Association

Swedish experiences

- Highly digitalised economy
  - 99,4% (18–67 years) use a BankID*
  - 95% (15–65 years) have the Swish** app downloaded on their mobile, thus enabling money transactions over the phone
  - The latest reported bank robbery was in 2020
- Personal data is public online
- Huge wave of **online fraud**
  - ‘Vishing scams’ reported to the police have increased by **555 %** since 2019
  - **Social engineering** methods
    - Manipulating the consumer to execute the transactions themselves

- The pendulum is now swinging back, with societal calls for **slowing down** some of the clients’ transactions, or at least for banks to provide for such options

* BankID is the eID dominating the Swedish market. In use since 2003. In April 2010 the mobile version was launched.

** Swish is the Swedish app for payments over the mobile phone between private users, to companies and for e-commerce. Launched in December 2012.

Our four pillar strategy

1. Strengthen society's defence system

- Stricter access to public information about individual's income, addresses etc.
- No spoofing of telephone numbers
- Information campaigns
- Fast digital reporting of fraud
  - Create the possibility for victims to report crimes to the police online
- Police need to investigate the crime clusters
- Central money mules register
- Reduce mules' ability to move money
- Social media platforms need to identify and eliminate fake accounts and misleading ads
- Strong formal requirements must be placed on accounting consultants to prevent companies from being used as criminal tools by criminals

2. Strengthen customers' security

- Customer protection
  - Time delays for certain transactions and amount limits for payments
    - Changes to these in a secure manner
  - Extra controls when making payments
    - For example, through a notification that informs the customer about the transaction or that the transaction must be approved by a person trusted by the customer
- Customer choice between availability and level of security
- Ability for banks to globally block the use of Swish and BankID by fraudsters and money keepers

3. Information sharing

- Fast digital reporting of fraud opens up for fast information sharing and mapping local mule registers between the banks
- AMLR (art. 54b and 54 [5]) gives new possibilities for data sharing 2027
  - Create private/private partnership, share information on customers and suspect transactions
  - Create permanent public/private partnership, share information on customers, suspect transactions etc
  - Information sharing between banks relating to a transaction – no longer a requirement that the sender and receiver of the transaction are the same person

4. Cooperation between banks and the police

- A new law enabling 'Special cooperation' in effect
  - A possibility for the FIU to create temporary partnerships ('4a') with banks to exchange e.g. information on customers and suspicion of money laundering and fraud
- Samlit (Swedish Anti-Money Laundering Intelligence Task Force)
  - The participating banks and The Swedish Bankers' Association jointly and regularly meet with the Swedish Police, National Operational Department, to prevent financial crimes such as money laundering, fraud and the financing of terrorism

Banks’ package of measurements, presented in May this year

- The requirements in PSD2 on strong customer authentication has led to a decrease in unauthorised transactions
  - From 50% to 10-15%
- 85-90% of the frauds are now performed through social manipulation

- **SBA’s package of measurements, in the form of recommendations to its members**
  - Stronger security at the expense of accessibility
    - Time delays for certain transactions, and amount limits for payments for different client categories
    - Extra controls when making payments falling out of the regular pattern for different client categories
    - Customers’ own choice of security level compared to accessibility
  - Block criminals from the financial system
    - Global blocking of Swish and BankID
    - Building and sharing mule register
    - Away with extra services – only fulfill the basic legal obligation for an account

- **FIU and police now reorganising** their work against fraud and money laundering, and their cooperation with banks

Looking ahead: new regulations increase the risk for fraud

Instant Payment Regulation (IPR)

- Requires payments to be made in **ten seconds**
- Opportunities to have delays and limitations on the size of transfers, **but** at the same time these limitations should be able to be lifted with **immediacy**

The Payment Services Regulation (PSR)

- The proposal on payment service provider's **liability for impersonation fraud**, when the fraudster for instance is pretending to be a bank employee, will support the criminal business model and could EU citizens more vulnerable to this type of fraud
  - A refund right for authorised transactions can make payment service users less concerned about security or lead to an increase in **'friendly fraud'** where the customer claims to be exposed to fraud, but in reality, is in collusion with the fraudster
- Definition of **authorisation** in PSR
  - The current policy discussion around the definition of authorisation would create legal uncertainty and fragmentation in EU payments regulation, undermining the well-established civil liability framework between payment service providers and payment service users
  - Introducing a subjective element for authorisation would enable payment service users' claim for a refund in any transaction, **undermining the need for risk assessment and control**