Implementation of EBA’s Guidelines on the security of internet payments

29-30 October 2015, Dubrovnik

Damir Blažeković
Agenda

The views expressed in this presentation do not necessarily reflect the views of the Croatian National Bank

- Introduction and background
- Overview of EU initiatives and legislative development on the security of internet payments
- Overview of payment statistics and internet banking in Croatia
EU regulation on the security of internet payments

- “Recommendations for the security of internet payments” (ECB Recommendations)

- “Final guidelines on the security of internet payments” (EBA Guidelines)

- “Payment Services Directive” (PSD2)
Main drivers

- Rising level of fraud observed on internet payments
- Security concerns among EU citizens
- CNP frauds have become the most prevalent type of payment frauds
- Too long period of time for transposition of the PSD2
- “Worrying” figures from EU reports on frauds:

[Images of EU reports on frauds]
Fourth Report on Card Fraud (ECB) -CNP frauds-

- Total value of card fraud ~1.44 billion EUR
- Total value of CNP fraud ~958 million EUR
- CNP fraud accounted for 66% of the total value of card fraud

<table>
<thead>
<tr>
<th>Year</th>
<th>CNP (EUR millions)</th>
<th>Share of total fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>~600</td>
<td>~10%</td>
</tr>
<tr>
<td>2010</td>
<td>~650</td>
<td>~15%</td>
</tr>
<tr>
<td>2011</td>
<td>~700</td>
<td>~20%</td>
</tr>
<tr>
<td>2012</td>
<td>~750</td>
<td>~25%</td>
</tr>
<tr>
<td>2013</td>
<td>~800</td>
<td>~30%</td>
</tr>
</tbody>
</table>

## Evolution of card fraud

### 20 – Evolution of Card Fraud

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraudsters</td>
<td>Individuals</td>
<td>Teams</td>
<td>Local crime rings</td>
<td>Global crime rings</td>
<td>Global crime rings with decentralised organisation</td>
</tr>
<tr>
<td>Target</td>
<td>Consumers</td>
<td>Small retailers</td>
<td>Larger retailers</td>
<td>Banks Processors</td>
<td>Payment Industry</td>
</tr>
<tr>
<td>Leading fraud types</td>
<td>Lost/stolen, Intercepted</td>
<td>Domestic, counterfeiting/skimming</td>
<td>Identity theft, Phishing, Rudimentary data compromise</td>
<td>Cross-border data compromise, CNP fraud, 3D-Secure Fraud, ATM fraud, ID fraud</td>
<td>Cross-border data compromise, CNP fraud, ATM fraud, ID fraud, Pharming, Hacking</td>
</tr>
<tr>
<td>Type of cards targeted</td>
<td>Travel &amp; Entertainment cards</td>
<td>Premium credit cards</td>
<td>Mass market credit cards</td>
<td>All types: credit cards, debit cards, prepaid cards</td>
<td>All types: credit cards, debit cards, prepaid cards, banking accounts</td>
</tr>
<tr>
<td>Necessary resources</td>
<td>Opportunism</td>
<td>Rudimentary knowledge</td>
<td>Technical knowhow</td>
<td>Audacity, Technical expertise, Insider information, Global connections</td>
<td>Audacity, Technical expertise, Insider information, Global connections</td>
</tr>
</tbody>
</table>

Source: Visa Europe, PCM research.

**Source:** Card Fraud Report, Payments Cards and Mobile, 2015
Consumer’s Perception
- FIS Consumer Banking PACE Index -

The Index measures:
• performance gaps on 18 service expectations.
• indicates gaps between consumers expectations and bank performance

FIS conducted online research with 9,000 banked consumers in nine countries to produce the index.

Timeline

2011: Set up of SecurePay forum

31 Jan 2013: ECB published Recommendations for the security of internet payments (Final)

Summer 2014: Conversion of ECB Recommendations into EBA Guidelines

19 Dec 2014: EBA issued Final Guidelines on the security of internet Payments

2 June 2015: Council of the EU published its final compromise text of PSD 2

1 August 2015: Entry into force of EBA Guidelines

End 2015*: Entry into force of PSD 2

End 2016*: Submitting RTS on authentication and communication to EC (12 months of the date of entry into force of PSD2)

+ application of the security measures (18 months from the date of entry into force of the RTS)

End 2017*: Transposition of PSD 2 into national laws (24 months after the entry into force of PSD 2)

End 2016*: Submitting RTS on authentication and communication to EC (12 months of the date of entry into force of PSD2)

End 2017*: Transposition of PSD 2 into national laws (24 months after the entry into force of PSD 2)
ECB Recommendations

- Developed by European Forum on the Security of Retail Payments (*SecuRe Pay*)
- Published by ECB on 31 January 2013.
- Entry into force originally was expected by 1 February 2015.
- In summer 2014 conversion of ECB Recommendations into EBA Guidelines was agreed.
- The conversion is intended to provide:
  - a more solid legal basis to ensure a consistent implementation by financial institutions across all MS
  - to provide confidence to financial institutions that the required investments and system changes are not carried out in vain.
- In December 2014 ECB Recommendations are superseded by EBA Guidelines.
- Addressees:
  - Payment Service Providers (PSPs)
  - Governance Authorities (GAs) of payment schemes
- “Comply or explain” principle (for PSPs):
  - Addressees are expected to comply with recommendations or need to be able to explain and justify any deviation from them upon the request of the relevant competent authority
EBA Guidelines

- **Issued** in December 2014 pursuant to Article 16 of Regulation (EU) No 1093/2010 which stipulates that competent authorities and financial institutions must make every effort to comply with the guidelines.

- **Entered into force** on 1 of August 2015

- **Do not affect** the validity of the ECB Recommendations

- **Establish** a set of minimum requirements in the field of the security of internet payments/internet payment services.

- **Apply to** the provision of payment services offered through the internet by PSPs as defined in Article 1 of the PSD1.
  - References to payment schemes, their Governance Authorities (GAs) have not been incorporated in the EBA Guidelines (as payment schemes are not covered by PSD1).

- **“Comply or explain” principle (for national authorities):**
  - National authorities had to notify the EBA within 2 months of the publication of the translations whether they will comply with the Guidelines or explain their reason for non-compliance.
    - 2 NA **complied partially** (Sweden, Cyprus)
    - 4 NA **did not comply** (Estonija, Slovakia, United Kingdom, Island)
EBA Guidelines

- In May 2015 CNB confirmed compliance with *EBA Guidelines*

- In May 2015 CNB published (on its web site):
  - **Translation** of *EBA Guidelines on the security of internet payments*
  - **Circular letter** about implementation of *EBA Guidelines*
    - CNB expects full implementation of the *EBA Guidelines* from the institutions under its jurisdiction.
EBA Guidelines

General control and security environment
- Governance
- Risk assessment
- Incident monitoring and reporting
- Risk control and mitigation
- Traceability

Specific control and security measures for internet payments
- Initial customer identification
- Strong customer authentication
- Provisioning of authentication tools
- Transaction monitoring
- Protection of sensitive payment data

Customer awareness, education and communication
- Customer education and communication
- Setting of limits
- Access to information about payment status
EBA Guidelines

**In scope:**
- **Cards** - card payments on the internet, including virtual card payments as well as the registration of card payment data for use in ’wallet solutions
- **Credit transfers** - credit transfers on the internet (internet banking)
- **E-mandate** - the issuance and amendment of direct debit electronic mandates;
- **E-money** - transfers of electronic money between two e-money accounts via the internet

**Out of scope:**
- other internet services provided by a PSP via its payment website (e.g. e-brokerage, on-line contracts)
- mobile payments other than browser-based payments
- credit transfers where a third party accesses the customer’s payment account
- payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology
- payment transactions made by an enterprise via dedicated networks;
- card payments using anonymous and non-rechargeable physical or virtual pre-paid cards where there is no ongoing relationship between the issuer and the cardholder
In June 2015 **Council of the EU** published its final compromise text for the new Payment Services Directive (PSD2) proposed by **European Commission** which aims to repeal and replace the Payment Services Directive (PSD1).

**PSD2 should:**
- **Improve consumer protection against fraud**, possible abuses and payment incidents through enhanced security requirements that make strong customer authentication for online payments compulsory and
- **Promote competition** through a regulatory framework conducive to the emergence of new players and the development of innovative mobile and internet payments in Europe.

**Third party providers (TPPs)** of account information and payment initiation services are in the scope of PSD2.

PSD2 encompass additional requirement **when the payer initiates electronic remote payment transaction** (art. 87). In that case PSPs should apply strong customer authentication that shall include elements dynamically linking the transaction to a specific amount and a specific payee.
PSD2 tasks EBA with the development of guidelines and technical standards on security aspects regarding payment services and strong customer authentication.

- **Management of operational and security risks (Art. 85)**
  - EBA shall, in close cooperation with the ECB develop Guidelines on security measures

- **Incident reporting (Art. 86)**
  - EBA shall, in close cooperation with the ECB develop Guidelines on incident reporting

- **Authentication (Art. 87)**
  - EBA shall, in close cooperation with the ECB develop draft Regulatory technical standards (RTS) addressed to PSPs specifying: the requirements of the strong customer authentication procedure, the exemptions to the application, the requirements that security measures have to comply with, the requirements for common and secure open standards of communication …..
**Internet banking in Croatia**

### 2FA:
- All banks in Croatia use 2-factor authentication
- Legally mandated since 2007.

<table>
<thead>
<tr>
<th></th>
<th>Retail</th>
<th></th>
<th>Corporate</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number trx.</td>
<td>Amount</td>
<td>Number trx.</td>
<td>Amount</td>
</tr>
<tr>
<td>Internet banking</td>
<td>32,66%</td>
<td>33,89%</td>
<td>51,40%</td>
<td>54,61%</td>
</tr>
<tr>
<td>Mobile banking</td>
<td>9,07%</td>
<td>7,52%</td>
<td>0,77%</td>
<td>0,14%</td>
</tr>
<tr>
<td>All e-channels</td>
<td>42,48%</td>
<td>46,36%</td>
<td>87,25%</td>
<td>92,98%</td>
</tr>
</tbody>
</table>

Source: Websites of various Croatian banks

Source:
Internet banking in Croatia
-IB transaction - (31/12/2014)-

**Enterprises:**
- Number of transactions: 6.29 mil.
- Value of transactions: 81.39 mlrd. HRK
- Number of IB users: 202,436

**Consumers:**
- Number of transactions: 3.47 mil.
- Value of transactions: 1.2 mlrd.HRK
- Number of IB users: 1,196,393

Source:
CNP transactions  
(31/12/2014)

- Number of CNP transactions: **1,7 mil.**
- Value of CNP transactions: **496,7 mil HRK**
- CNP transactions accounted less than 1% in total number of national card payment transactions.

Source: HNB, Platne kartice i kartične transakcije, 2014.
Internet banking fraud in Croatia
- Many insiders’ viewpoint until 2014 -

- Has not happened for nearly 20 years…

- Will never happen because:
  - …our banks’ internet banking is completely secure,
  - …we are too small to be interesting to international hackers,
  - … it’s not cost-effective to build customized malware and infrastructure for:
    - our internally developed internet banking application,
    - our specific payment systems,
    - in Croatian language,
    - money transfer via money mules.

But …
Since 2014.
Internet banking fraud attempts
- nr. of trx. & amount / month -

Source: Internet banking fraud incidents reported to the CNB in 2014 and 2015
Attacks are...

- Well researched and prepared:
  - Good understanding of Croatian payments landscape;
  - Fake websites are well prepared and quick to adapt to changes;
  - Good (continually improving) command of Croatian language;
  - Wide recruitment of money mules
    - http://www.mup.hr/208020.aspx

- Structured and organized.

- Obviously, a lot of effort was put into devising and performing them.

- Not going to be simple to deter.
Relevant regulatory framework, standards and guidelines

- **Payment system act** (Official Gazette 133/2009, 136/2012)
  - Titels I – III

- **Publication of Announcement** regarding public interest in issues related to the abuse of electronic banking *(May 2014)*

- **EBA - Final guidelines on the security of internet payments** *(May 2015)*
  - Notification sent to EBA (confirmation of compliance with EBA Guidelines)
  - Publication of *Circular letter* about implementation of EBA Guidelines

- **Decision on adequate information system management** *(Official Gazette 37/2010)*
Thank you for your attention!

Questions, comments...