NATIONAL BANK OF ROMANIA

Rolul băncii centrale în salvgardarea plăților inițiate prin instrumente de plată

11 iunie 2015

Responsabilități și competențe ale BNR în domeniul plăților de retail

Legea 312/2004 privind statutul BNR

Atribuții

- promovarea şi monitorizarea bunei funcţionări a sistemelor de plăţi pentru asigurarea stabilităţii financiare

Competențe

- Banca Naţională a României monitorizează sistemele de plăţi, inclusiv instrumentele de plată, în scopul asigurării securităţii şi eficienţei acestora
- poate reglementa instrumentele de plată

Atribuții ale băncilor centrale din SEBC

Atribuții convergente

- Promovarea bunei funcţionări a sistemelor de plăţi (Art. 127 alin. (2) Tratatul privind funcționarea Uniunii Europene)

Atribuții divergente

- Responsabilități privind protecția consumatorilor – Italia,Portugalia, Cehia, Slovacia, Slovenia, Spania, etc
- BNR implicată tangențial și în protecția consumatorilor - activitatea BNR de identificare și evaluare a riscurilor care pot să apară pe parcursul decontării tranzacțiilor de plată, începând de la inițiere și până la creditarea sumei de bani care face obiectul acestor tranzacții în contul clientului
- Cadru comun de supraveghere a acestor plăți în Uniune
    - băncile centrale din SEBC au identificat o serie de riscuri și
    - au elaborat standarde de oversight (supraveghere)

Riscul de fraudă

Activitatea de supraveghere a băncii centrale

- **Subiect** – autoritatea de guvernanța a schemei de plăți (AG) și PSP
- **Obiect** funcţionarea sigură a sistemului de plăţi/schemei de plăți
- **Componente**
  - Monitorizare (informații publice, documente oficiale ale schemei de plăți, raportări, etc.)

    Dezvoltarea cadrului legal necesar în activitatea de monitorizare – noi indicatori
  - Evaluare - modul în care este administrat riscul de fraudă în cadrul schemei
  - Inducere de schimbări

Evaluarea activității de administrare a riscului de fraudă

- Autoritatea de guvernanță stabilește obligațiile specifice ale PSP privind administrarea riscului de fraudă
- PSP trebuie:
    1. să realizeze **evaluări periodice ale riscurilor** specifice pentru activitatea de plăți desfășurată actualizate permanent în funcție de evoluțiile înregistrate în mecanismele de detectare a fraudei
    2. să implementeze proceduri eficace de **autorizare a tranzacțiilor și de monitorizare** a acestora
    3. să implementeze o procedură prin care **clienții sunt informați** (printr-un canal securizat) cu privire la **actualizările** aduse de acesta procedurilor de securitate și prin care se transmit alerte cu privire la riscurile semnificative determinate de evenimente în curs de desfășurare (de ex. de tip social-engineering)
    4. **să informeze clienții** despre modul în care se utilizează instrumentele procesate în cadrul schemei și **măsurile de securitate** care pot fi luate de către aceștia în scopul prevenirii fraudei (cum ar fi să seteze limite pentru tranzacțiile efectuate, să ia măsuri pentru blocarea serviciului/a unei tranzacții specifice în cazul în care există o suspiciune de fraudă).

Evaluarea activității de administrare a riscului de fraudă

6. să implementeze **programe de educare** a clienților care să vizeze:
    - Conștientizarea necesității de protecție a
        - ✓ elementelor harware și software utilizate de către clienți pentru asigurarea securității tranzacțiilor de plată, (aceasta înseamnă că utilizatorii de servicii de plată ar trebui să protejeze elementele de identificare și autentificare în raport cu prestatorul de servicii de plată (credențiale, token-uri, etc) să-și protejeze computerele personale prin utilizarea și actualizarea unor programe specifice cu caracter de protecție (antivirus, firewall, security patches etc.)
        - ✓ a datelor confidențiale/ sensibile (informații care ar putea fi utilizate pentru a realiza o fraudă) și a altor date personale ale acestora.
    - conștientizarea necesității de a nu minimaliza riscurile potențiale la care se expun în cazul în care decid să descarce din mediul internet programe cu privire la care nu au, în mod rezonabil, certitudinea că sunt sigure, originale și că nu au fost alterate
    - să acorde o atenție sporită identificării **site-ului real/oficial** al prestatorului de servicii de plată

Evaluarea activității de administrare a riscului de fraudă

6. Să explice clienților lor

   ✓ procedura de **raportare a tranzacțiilor suspecte sau frauduloase**, incidentele sau anomaliile cu care s-au confruntat încercând să efectueze o plată pe internet

   ✓ modul în care clientul urmează să i**nteracționeze** cu prestatorul său de servicii de plată

   ✓ modul în care prestatorul său de servicii de plată îl **informează cu privire la o tranzacție frauduloasă** sau care are acest potențial sau despre faptul că o tranzacție de plată nu a fost inițiată

✓ modul în care prestatorul său de servicii de plată î**l informează** cu privire la existența **unor amenințări** (de ex. a unui atac de tip phising în desfășurare)

Vă mulțumesc pentru atenție!

Denisa Iatan, Direcția Stabilitate Financiară

Detalii de contact: Str. Doamnei, nr. 8, București, România
T: +4031 132 1152 F: +4021 313 0654 E: denisa.iatan@bnro.ro
www.bnr.ro