7. SISTEMELE DE PLATĂ PENTRU COMERȚUL ELECTRONIC ŞI VULNERABILITĂȚILE ACESTORA

Apariția comerțului electronic a generat nevoia de noi servicii financiare ce nu puteau fi pe deplin puse practică prin intermediul serviciilor tradiționale de plată. În această situație, toate părțile interesate au căutat soluții pentru un sistem electronic de plată viabil. În linii mari sistemele electronice de plată existente pot fi grupate în 4 categorii:

- Sisteme de plată on-line pe bază de carduri bancare
- Sisteme de plată on-line bazate pe numerar digital şi
- Sisteme de cecuri electronice.

Fiecare sistem electronic de plată prezintă atât avantaje cât şi dezavantaje pentru consumatori şi comercianți.

7.1. Conceptul de plată electronică şi dimensiunile sale

Sistemele de plăți care folosesc rețelele electronice de distribuție sunt utilizate frecvent în domeniile bancar şi de afaceri încă din 1960, în special pentru transferul unor sume mari de bani. Cele peste cinci decenii ce au trecut de la apariția lor au fost pline de dezvoltări tehnologice; acestea, pe de o parte, au contribuit la expansiunea sistemelor electronice de plăți, iar pe de altă parte, au creat noi activități şi practici sociale ce au făcut indispensabile aceste sisteme. Aceste schimbări au afectat modul în care sunt definite plățile electronice. Într-o formă generală, termenul de plată electronică se referă la orice fel de plată către mediul de afaceri, bănci sau administrația publică realizată de persoane fizice sau juridice prin intermediul telecomunicațiilor sau rețelelor electronice. Este evident că plecând de la această definiție, tranzacțiile sunt realizate între părți fără intervenția fizică a vreunei alte persoane. În afară de aceasta, plata este realizată de la distanță, fără prezența fizică a plătitorului şi, fireşte, fără a se folosi numerar.

Sistemele de plăți electronice sunt folosite în toate formele de comerț electronic: B2B, B2C, C2C, B2G, C2G fiecare având particularități depinzând de valoarea tranzacției. Danial[1], clasifica sistemele electronice de plăți după cum urmează:

- Microplăți a căror valoare nu depăşeşte 10 USD utilizate în comerțul electronic C2C şi B2C
- Plăți de consum a căror valoare este cuprinsă între 10 şi 500 USD, întâlnite în special în tranzacțiile B2C, C2G
- Plăți de afaceri a căror valoare depăşeşte 500 USD, utilizate în tranzacțiile B2B şi B2G.

Tranzacțiile B2B au un volum de 95 % din totalul tranzacțiilor efectuate, în timp ce restul au o pondere de doar 5 %.[2]

Sistemele electronice de plăți care operează cu plăți de mică valoare trebuie să găsească un echilibru între comoditatea tranzacției (a cărei asigurare generează cea mai mare parte a costului în cazul acestui tip de tranzacții) şi securitatea sa. Pe de altă parte, tranzacțiile cu valori mari necesită protocoale de securitate mai înalte a căror implementare este costisitoare. În final, aproape toate sistemele electronice de plăți pot efectua tranzacții cu sume de valori medii.

Sisteme convenționale vs. sisteme electronice de plăți

Un proces de plată convențional implică un transfer de numerar sau informații legate de plată (de exemplu, în cazul cecurilor sau cardurilor bancare) între cumpărător şi vânzător. Acest transfer are loc în rețeaua de procesare a băncilor. O plată efectuată cu numerar presupune o retragere de bani din contul bancar al cumpărătorului, transferul fizic al sumei către vânzător, iar în final depunerea sumei de către vânzător în contul său. Mecanismele de plată fără numerar implică creditarea şi debitarea unor conturi bancare pe baza informațiilor transmise prin intermediul cecurilor sau cardurilor bancare.

Numerarul este transferat de la banca cumpărătorului la banca vânzătorului prin intermediul unui schimb fizic realizat în piață. Dacă se apelează la o metodă de plată fără numerar, vor fi transferate informații vizând plata între cumpărător şi vânzător, în locul

---

[1] Danial, A., *E-Business (R) evolution,* Prentice Hall, New York, 2002

[2] Turban, E., King, D., Jae Kyu L., Viehland D., *Electronic Commerce: A Managerial Perspectiv*e 2006 *(4th Edition)*, Prentice Hall, 2005

transferului de numerar; în final plățile sunt realizate între băncile implicate, acestea ajustând în final conturile vânzătorului, respectiv cumpărătorului pe baza informațiilor vizând plata.

Sistemele electronice de plăți au început să funcționeze din 1960, începând să se extindă şi să-şi dezvolte complexitatea. Transferul electronic de fonduri (EFT- Electronic Fund Transfer) a fost primul sistem electronic de plăți, ce nu depindea de o entitate intermediară de procesare. Transferul electronic de fonduri este o aplicație a tehnologiei EDI; acest instrument financiar asigură transmisia între bănci şi firme, prin intermediul rețelelor securizate, a informațiilor legate de carduri sau cecuri electronice. Totuşi pentru a utiliza transferul electronic de fonduri la efectuarea de plăți şi ajustarea în concordanță a conturilor bancare, trebuia adăugat un serviciu de plată on-line cu rolul de a asigura procesarea ordinelor de plată şi efectuarea modificărilor în conturile bancare. Un jalon în acest sens a fost pus odată cu dezvoltarea numerarului digital. Acesta, având la bază şiruri de biți, poate fi transportat pe un smart card sau poate fi păstrat pe un calculator personal. La fel ca în cazul cecurilor de călătorie, numerarul digital reprezintă o creanță flotantă către o bancă sau o altă instituție financiară, nefiind legată de un anumit cont bancar.

Prin natura sa, numerarul digital este o oglindire a banilor din hârtie ca mijloc de plată. Ca atare, sisteme de plată bazate pe numerarul digital oferă aceleaşi avantaje ca şi sistemele de plăți bazate pe bani din hârtie, şi anume în primul rând, anonimitatea şi confortul.

În figura 2 este prezentată schema unui sistem de plată cu numerar digital.

Fig. 2 Sistem electronic de plată

Se observă existenţa două fluxuri şi anume: cel al numerarului fizic, respectiv cel al numerarului virtual. În timp ce numerarul fizic este reprezentat de transferuri de bani, numerarul virtual este reprezentat atât de dispozitive electronice (token-uri, smart carduri), cât şi de aplicaţii informatice (e-cash, e-cheque). Elementul de legătură între cele două fluxuri îl constituie o instituţie mediatoare, ce acţionează ca o bancă electronică, rolul său fiind acela de a converti numerarul fizic în numerar virtual şi reciproc. Instituţia mediatoare este de regulă un furnizor de servicii de sine-stătător (ex: GECAD, ROMCARD etc.).

Sistemele de plată cu numerar digital au un larg impact asupra banilor şi sistemelor monetare, cu implicaţii extinse mult dincolo de cele vizând tranzacţiile. Practic apariţia acestor sisteme a condus la apariţia şi dezvoltarea unor domenii conexe, cum ar fi cel al soluţiilor software pentru sistemele de plăţi, pentru securitatea tranzacţiilor, pentru criptarea/decriptarea datelor şi pentru autentificarea părţilor, cel al serviciilor bancare de interfaţă între numerarul virtual şi cel fizic, cel al dispozitivelor hardware (token-uri, smart carduri, citoare de carduri etc.).

7.2. Tipologia sistemelor de plăți electronice

Odată cu creşterea complexităţii tranzacţiilor de comerţ electronic, au apărut diferite sisteme de plăţi electronice. Ele pot fi grupate în funcţie de tipul informaţiei transferate on-line. Murthy[3] identifică şase sisteme de plăţi electronice:

1. PC Banking
2. Cardurile bancare
3. Cecurile electronice (i-cheques)
4. Microplăţile
5. Cardurile cu cip (smart card)
6. E-numerarul (e-cash).

Anderson împarte sistemele electronice de plăţi în:

- Sisteme de plăţi on-line cu card bancar
- Sisteme cu cecuri electronice
- Sisteme de electronic banking
- Sisteme cu numerar electronic (digital)

Sistemele de plăţi cu card bancar. Caută să extindă funcţionalitatea cardurilor bancare cu bandă magnetică prin utilizarea acestora ca instrumente de plată pentru cumpărăturile efectuate on-line. Acest instrument de plată este acceptat pe scară largă de consumatorii şi comercianţii din întreaga lume şi este, de departe, cea mai populară metodă de plată îndeosebi pe piaţa de retail. Această metodă de plată are o serie de avantaje, ce nu se regăsesc la metodele clasice de plată. Cele mai importante sunt: confidenţialitatea, compatibilitatea, eficienţa ridicată a tranzacţiei, acceptabilitatea largă, comoditatea, mobilitatea, riscul financiar relativ redus şi anonimatul. În plus faţă de acestea, pentru a evita complexitatea caracteristică numerarului digital sau cecurile electronice, consumatorii şi vânzătorii au văzut în plăţile cu card bancar pe Internet o

---

[3] Murthy, C.S.V., *E-Commerce: Concepts, Models and Strategies*, Himalaya Publishing House, New Delhi, 2002

soluție viabilă, testată de-a lungul timpului. Dar acest sistem de plată a ridicat o serie de probleme consumatorilor şi comercianților printre care pot fi enumerate: lipsa autentificării, contestarea plăților şi fraudele cu carduri bancare. Mai trebuie menționată teama consumatorilor de a utiliza cardurile bancare pe Internet generată de necesitatea de a dezvălui informații despre acestea pe mai multe site-uri şi de a comunica în mod repetat informații sensibile prin Internet.

Cel mai uzual şi simplu mod de efectuare a transferului electronic de fonduri este acela de a utiliza un card bancar pentru a extrage numerar sau a efectua plăți prin intermediul unui ATM, pentru a plăti contravaloarea unor produse sau servicii prin intermediul unui sistem POS (Point Of Sale) sau la plata unor produse comandate prin Internet.

Principalele operații ce pot fi efectuate prin intermediul card-ului bancar sunt:

- Plata directă la comerciant a unor bunuri/servicii
- Rambursarea de către comercianți a unor sume de bani, datorită imposibilității acestora de a livra produsele sau serviciile solicitate
- Retragerea de numerar, de regulă prin intermediul unui ATM
- Alimentarea unui cont de card fie de la ghişeele băncii emitente, fie prin serviciul de e-banking
- Plata efectuată prin transferul în contul unei terțe părți (exemplu plata prin ATM a facturilor de energie electrică, gaze, telefonie etc.)
- Interogarea contului de card şi/sau solicitarea unui miniraport cu operațiile efectuate din contul de card
- Operații administrative cum ar fi solicitarea schimbării PIN-ului.

Operațiile oferite clienților diferă de la o bancă la alta, variind însă şi în funcție de terminalul utilizat (de exemplu operațiile ce pot fi efectuate la un ATM diferă de cele realizate la un POS).

Pentru a efectua o plată trebuie ca aceasta să fie autorizată de banca emitentă. Când un card bancar este folosit la un comerciant sau un ATM, tranzacția este întâi direcționată către procesatorul de plăți electronice şi apoi către banca emitentă.

În majoritatea cazurilor tranzacția este efectuată on-line în timp real, intervalul de timp scurs între solicitarea efectuării unei plăți din contul de card şi autorizarea acesteia este de ordinul zecilor de secunde.

Tranzacțiile pot fi realizate şi off-line între oricare din entitățile implicate în proces, pe baza unui acord între părți. Această modalitate de efectuare a tranzacției poate fi folosită atunci când linia de comunicație nu este disponibilă, sau pur şi simplu pentru a reduce costurile aferente. În cazul acestui tip de tranzacții, în acord sunt menționate limitele de siguranță. Limitele de siguranță sunt calculate pe baza riscului pe care le implică autorizarea off-line a unei tranzacții şi de aceea, ele variază în funcție de tipul cardului şi de comerciant.

În cazul tranzacțiilor off-line se apelează la elemente suplimentare de siguranță precum: compararea seriei cardului cu seriile cardurilor furate, limitarea numărului de tranzacții ce pot fi efectuate off-line cu un card şi la realizarea în mod aleatoriu a unora dintre tranzacții on-line.

O tranzacție poate fi autorizată şi în două etape. În prima etapă, aceea de preautorizare, comerciantul cere băncii emitente să rezerve o anumită sumă de bani pentru un interval de timp prestabilit, iar în cea de-a doua, numită etapă de finalizare, comerciantul retrage contravaloarea bunurilor /serviciilor. Acest tip de tranzacții este adesea utilizat în domeniul hotelier, al închirierii de maşini şi în alte situații similare, în care nu se cunosc costurile finale ale serviciilor oferite, pre-autorizarea realizându-se pe o sumă estimată.

O altă componentă importantă a tranzacției prin card bancar este autentificarea cardului şi a posesorului său. Pentru realizarea acestei operații sunt disponibile următoarele variante:

- Cea mai simplă presupune verificarea semnăturii posesorului de card
- A doua variantă este aceea a numărului personal de identificare (PIN), care, odată introdus de posesorul cardului, este transmis on-line în formă criptată băncii emitente

A treia variantă, folosită în special la tranzacțiile la care cardul nu este prezentat (ex: magazine virtuale) este aceea a introducerii codului de securitate a cardului (Card Security Code – CVV2) imprimat fie pe fața cardului, fie pe spatele său.

- Ultima variantă nu implică nici o intervenție umană şi se realizează automat la citirea informațiilor de pe banda magnetică a cardului cu un cititor de carduri (de exemplu, cel al unui POS).

Datorită problemelor de securitate[4] pe care le implică plățile prin Internet efectuate cu cardurile bancare, Visa şi Mastercard au introdus sistemul antifraudă 3D Secure. Acesta reuneşte tehnologiile ce stau la baza protocoalelor „Verified by Visa" respectiv „Mastercard Secure Code".

Folosirea sistemului 3D Secure permite creşterea securității tranzacțiilor on-line, prin solicitarea unei parole la fiecare plată on-line. În caz de pierdere sau furt, cardul înrolat la 3D Secure, nu poate fi folosit de terțe persoane pentru cumpărături on-line. Se elimină astfel riscul fraudei prin copierea informațiilor de plată sau prin generarea aleatoare de numere de carduri şi utilizarea lor ulterioară pe Internet. Prin folosirea acestui sistem de tranzacționare se aşteaptă o reducere a disputelor din fraudele rezultate din tranzacțiile on-line cu cel puțin 80%.

În țara noastră serviciul este disponibil la doar o parte din bănci: BCR, Raiffeisen, Unicredit, BRD, Alpha Bank, Romexterra, CEC, Banca Transilvania, ATE Bank, RIB si ING Bank. De asemenea nu pentru toate tipurile de carduri bancare emise de aceste bănci acest serviciu este disponibil.

Comercianții care au implementat acest sistemul de comerț electronic securizat pot fi identificați după siglele "Verified by VISA" sau "MasterCard Secure Code" (figura 4) afişate pe site-urile lor.

Fig. 4. Siglele care certifică implementarea sistemului 3D Secure

[4] de exemplu, în cazul în care o persoana rău-voitoare deține informațiile de card (număr, data expirare, cod CVV), poate plasa comenzi în mediul on-line.

Pentru activarea unui card în sistemul 3D Secure trebuie accesat link-ul corespunzător de pe site-urile băncilor. Se cer câteva informații referitoare la cardul bancar, după care trebuie introduse informații care vor fi personalizate, dar şi o parola pe care setată personal de posesorul cardului. Spre exemplificare vor fi prezentați în cele ce urmează paşii necesari pentru activarea acestui serviciu la o banca imaginară numită Banca Ta. Majoritatea băncilor au o procedură de activare relativ asemănătoare celei prezentate în continuare.

Se accesează interfața de activare a 3D Secure a băncii. Prima pagina a interfeței este prezentată în figura 5. Pentru a începe activarea, se apasă butonul "*Continuare*".

VERIFIED by VISA

BANCA TA

Protejati-va cardul Visa pentru tranzactii pe INTERNET

Cardul dvs. Visa a fost inregistrat **gratuit** la serviciul "*Verified by Visa*", pentru a va proteja de utilizarea neautorizata pe Internet.

De indata ce veti activa serviciul e-commerce BT, banca dvs. va solicita parola personala (pentru plati pe Internet), ori de cate ori veti face o plata la magazinele virtuale inregistrate Verified by Visa.

Inainte de a continua va rugam sa cititi **Regulile si conditiile de utilizare** (mai jos) a serviciului e-commerce BT. **Selectare optiunii "Continuare" este considerata a fi acordul dvs. pentru regulile si conditiile mentionate.**

Pentru a obtine parola dvs. personala pentru plati pe internet este nevoie sa cunoasteti parola initiala de inrolare.

Parola initiala de inrolare este compusa din: ultimele 6 cifre din CNP-ul dvs. + ultimele 6 cifre din numarul cardului.

Continuare | Nu activa acum

English version

Prin apasarea butonului *Continuare*, sunteti de acord cu Regulile si conditiile de utilizare

Fig.5. Prima pagină a interfeței de activare

Pasul 1. Trebuie completat formularul din figura 6, cu următoarele date:

- Numărul cardului
- Data expirării
- Codul numeric personal (CNP)
- Parola inițială depinde de condițiile impuse de fiecare bancă în parte. De exemplu, parola inițială poate fi formată din ultimele 6 cifre ale CNP-ului şi ultimele 6 cifre din numărul cardului.

După completarea formularului, se apasă butonul „*Continuare*” pentru a trece la pasul 2.

Fig.6. Interfața pentru autentificarea posesorului de card

Pasul 2. În figura 7 este prezentată fereastra în care este activate efectiv cardul, în modul următor:

- Utilizatorul îşi stabileşte un nume de utilizator. Trebuie să fie format din minim 4 caractere şi nu poate avea decât cifre sau litere şi cel mult un spațiu. Trebuie să

fie uşor de reţinut, pentru că este posibil să mai fie necesar pentru eventuale verificări ulterioare (de exemplu, la regenerarea parolei)

- Se stabileşte parola. Aceasta este parola 3D Secure ce va folosită doar la efectuarea cumpărăturilor on-line. Fără a cunoaşte aceasta parola, nicio persoană nu va putea folosi cardul pentru cumpărături on-line. Parola 3D Secure trebuie să conţină între 8 şi 14 caractere, minim 1 cifră şi 1 literă, fără alte caractere speciale. *Este foarte important ca această parolă să nu fie comunicată altor persoane.*
- Urmează stabilirea unui text care să ajute la reamintirea parolei 3D Secure în cazul uitării ei (de exemplu, un indiciu). Textul trebuie să conţină minim 4 caractere şi să fie diferit de parolă.
- În final, se stabileşte un mesaj de întâmpinare (ex: Bună ziua! Ce mai faceţi?) care va apărea automat în timpul procesului de plata on-line, atunci când se va cere parola 3D Secure. Acest mesaj trebuie să fie diferit de parola 3D Secure şi de textul de reamintire, iar scopul său este de a asigura utilizatorul că pagina de autentificare este găzduită de banca emitenta a cardului.

Fig.7. Interfața pentru definirea parametrilor personali necesari sistemului 3D Secure

După completarea tuturor câmpurilor se apasă butonul „Activați acum” şi va fi afişată o fereastră (figura 8) ce va indica activarea cu succes a setărilor pentru serviciul 3D Secure.

Fig.8. Fereastră indicând activarea serviciului 3D Secure

La efectuarea unei plăți on-line la comercianții care au implementat sistemul 3D Secure, după introducerea informațiilor referitoare la card în formularul de plată (vezi figura 3), apare până la finalizarea tranzacției o fereastră suplimentară cu interfața în care trebuie introdusă parola stabilită la activarea sistemului (figura 9).

Procesul de autentificare nu necesită instalarea vreunei aplicații speciale pe computerul clientului, nu îngreunează navigarea pe Internet şi determină creşterea încrederii în aceasta modalitate de a cumpăra bunuri/servicii.

Fig. 9. Exemplu de fereastră pentru validarea 3D Secure a unei plăți

Sistemul de plăți cu cecuri electronice. Acest sistem se adresează tuturor celor care astăzi folosesc cecurile tradiționale de hârtie pentru a efectua plăți către alți comercianți, consumatori sau către instituțiile statului. Sistemul de e-cecuri a fost creat pentru a funcționa într-un mod asemănător cecurilor convenționale de hârtie. Un posesor de cont va emite un document electronic ce conține numele instituției financiare, numărul contului din care este efectuată plata, numele beneficiarului şi suma. Cea mai mare parte a informațiilor sunt necodificate. Similar cecurilor din hârtie ele poartă echivalentul digital al semnăturii clasice: semnătura electronică ce un număr generat care certifică faptul că cecul este emis de posesorul contului. Sistemul de plăți cu cecuri electronice caută să extindă funcționalitatea sistemului tradițional pentru a putea fi utilizat ca un instrument pentru plata achizițiilor efectuate on-line. Sistemul de cecuri electronice are mute avantaje:

– Utilizatorii nu trebuie să dezvăluie informațiile despre cont altor persoane atunci când participă la o licitație

– Utilizatorii nu trebuie să transmită în mod continuu informații financiare sensibile prin Internet

– Sunt mai ieftine decât cărțile de credit

– Plata este efectuată mai rapid decât prin cecurile clasice de hârtie.

Dar acest sistem de plată are şi o serie de dezavantaje dintre care pot fi menționate: costurile fixe ridicate, utilizarea lor limitată doar la lumea virtuală şi faptul că nu pot proteja anonimatul utilizatorilor. De aceea sistemul de plăți cu cecuri electronice nu este foarte potrivit pentru vânzarea cu amănuntul către consumatorii finali, ci mai degrabă este util în cazul tranzacțiilor B2B sau B2G deoarece acestea nu necesită anonimat, iar sumele vehiculate sunt în general suficient de mari încât să depăşească cu mult costurile de procesare a cecurilor.

O tranzacție completă cu cecuri electronice constă dintr-o serie de paşi diferiți. Aceştia sunt executați în trei faze distincte, ce pot fi în unele cazuri separate între ele. Într-o primă fază consumatorul efectuează o cumpărare; în cea de-a doua fază, comerciantul trimite băncii sale cecul electronic în vederea efectuării plății. În cea de-a treia fază, banca comerciantului ia legătura cu oficiul de decontare sau cu banca cumpărătorului pentru a încasa cecul. În continuare vor fi prezentați concret paşii parcurşi la efectuarea unei tranzacții cu cecuri electronice (figura 10):

Fig. 10. Sistemul de clearing al cecurilor electronice

Pasul 1. Cumpărătorul completează un formular de comandă, ataşează un aviz de plată (cec electronic), îl semnează cu cheia sa privată (folosind dispozitivul electronic de care dispune în acest scop), ataşează certificatul cheii sale publice, îl criptează folosind cheia sa privată şi îl trimite vânzătorului.

Pasul 2. Vânzătorul decriptează informația folosind cheia sa privată, verifică certificatele, semnătura şi cecul cumpărătorului, ataşează avizul său de depunere şi andosează depunerea ataşând certificatul cheii sale publice. Acestea sunt criptate şi trimise către banca sa.

Pasul 3. Banca vânzătorului verific semnăturile şi certificatele şi trimite cecul pentru decontare. Oficiul de decontare şi băncile de regula sunt interconectate printr-o rețea privată securizată.

Pasul 4. Când cecul este decontat, suma este creditată în contul vânzătorului şi îi este trimis un aviz de creditare.

Pasul 5. Cumpărătorul primeşte un avizul de debitare

Cecurile electronice furnizează mediului de afaceri o modalitate sigură de plată prin Internet şi oferă o cale simplă de acces în lumea comerţului electronic, fără a fi necesară o investiţie majoră în noi tehnologii.

Sisteme de electronic banking (e-banking). Serviciile bancare electronice reprezintă serviciile bancare care pot fi puse la dispoziţia persoanelor fizice şi a companiilor de către o bancă prin mijloace electronice sau parţial electronice, în general, prin intermediul unui telefon fix sau mobil, dar şi prin Internet. Aceste servicii permit administrarea totală sau parţială a unui cont bancar, efectuată de deţinătorul contului, contul putând fi curent, la termen sau de card, fără a mai fi necesară deplasarea deţinătorului de cont la ghişeul băncii. Serviciile bancare electronice oferă acces la diverse informaţii de cont şi financiar-bancare, în general, şi pot permite efectuarea de transferuri de fonduri şi plăţi din cont. Deţinătorii de conturi pot avea acces la aceste servicii dacă se înregistrează la bancă în acest scop şi primesc, după acceptarea înregistrării, o modalitate de identificare unică (nume, parolă, PIN (Personal Identification Number), expresii de control (de exemplu, iTAN - Indexed Transaction Authentication Number), dispozitiv special(Token), care să le permită o utilizare sigură a serviciilor.

În general, electronic banking reprezintă, practic, un fel de "umbrelă" care acoperă întregul proces prin care un client poate să realizeze tranzacţii bancare pe cale electronică, fără a fi nevoie să se deplaseze la bancă. Următorii termeni se referă la o formă sau alta de e-banking: computerul personal (PC banking), utilizarea Internetului (Internet banking), banca virtuală (virtual banking), servicii bancare on-line, servicii bancare la domiciliu (home banking), servicii bancare la distanţă (remote electronic banking) şi telefonul (phone banking). Din punctul de vedere al comerţului electronic cele mai utilizate servicii bancare electronice sunt: computerul personal (PC banking) şi Internet banking-ul. Este necesar să menţionăm, totuşi, că termenii utilizaţi pentru a descrie diferitele tipuri de servicii bancare electronice sunt, adesea, utilizaţi concomitent.

– **PC banking-ul** reprezintă o formă de servicii bancare online care le dă clienţilor posibilitatea de a executa tranzacţii bancare de pe un computer via un modem. În acest caz, banca oferă clientului în proprietate un software financiar

care permite clientului să realizeze tranzacții financiare prin propriul său computer de acasă. În mod curent, multe bănci oferă sisteme de PC banking care permit clienților să obțină extrase de cont cu soldurile conturilor, note de plată şi transferuri de fonduri între conturi.

– **Internet banking**, uneori este denumit serviciu bancar on-line şi reprezintă este o formă mai avansată de PC banking. Internet banking utilizează Internetul ca şi canal de distribuție prin care se dirijează activitatea bancară, de exemplu;: transferarea fondurilor, plata facturilor, vizualizarea soldurilor conturilor de economii, plata ipotecilor şi cumpărarea instrumentelor financiare şi a certificatelor de depozit. Serviciile bancare de Internet sunt cunoscute ca fiind servicii virtuale (cyber net) interactive sau web-banks (web-site-urile băncilor).

Serviciile bancare prin Internet au, în general, costuri operaționale şi tranzacționale mai scăzute decât serviciile bancare obişnuite. Aceste servicii bancare nu sunt limitate numai la o locație fizică (physical site); uneori, există bănci Internet fără ca aceste bănci să aibă în mod fizic sucursale, cum ar fi, de exemplu, Telebank (Arlington, Virginia) şi Banknet (UK). Mai mult, în anumite cazuri, web-sit-urile băncilor nu sunt restricționate să-şi realizeze tranzacțiile în cadrul frontierelor naționale şi au capacitatea de a efectua tranzacții care implică sume mari de bani.

În general, serviciile bancare electronice, se pot clasifica în doua categorii:

a. furnizarea de informații şi, respectiv

b. efectuarea de transferuri de fonduri şi de plăți .

a. **Informațiile bancare** furnizate electronic de bancă sunt informații cu privire la contul bancar şi informații financiar-bancare generale, cum ar fi cele referitoare la cursul de schimb valutar, dobânzile sau comisioanele curente, rețeaua de ATM-uri, cele de utilitate generală.

Informațiile cu privire la cont se referă la: valoarea soldului contului curent, istoricul tranzacțiilor efectuate în şi din cont, situația extraselor de cont. Tot în categoria informațiilor bancare furnizate electronic se pot încadra şi mesajele SMS trimise de bancă deținătorului de cont de card, la momentul efectuării unei tranzacții cu cardul.

b. **Transferurile de fonduri** din cont pot fi transferuri intrabancare (contul

receptor e în aceeaşi bancă cu contul emiţător) sau interbancare.

Plăţile ordonate se pot efectua către un cont intrabancar (între clienţii băncii), către o alta bancă sau către trezorerii, în moneda ţării sau în altă monedă. Se poate ordona vânzarea sau cumpărarea de valută. O companie poate ordona plata salariilor către angajaţii săi, pornind de la un cont de salarii al companiei, către o listă prestabilită de conturi de salariaţi (care pot fi şi conturi de card). Se pot face plăţi de facturi şi de reîncărcare a cartelelor telefonice.

Fiecare bancă devenită e-bancă oferă unele dintre aceste servicii sau chiar pe toate, grupate pe pachete de servicii adecvate unor anumite canale de acces. Dacă accesul se face, de exemplu, prin SMS de la un telefon mobil, atunci, de regulă, se oferă numai informaţii, în vreme ce în cazul unui acces prin Internet pot fi disponibile toate serviciile, inclusiv plăţile şi transferurile.

Pentru a avea acces la toate aceste servicii, un deţinător de cont, persoană fizică sau companie, trebuie să se înregistreze la e-banca la care deţine contul. Ca urmare a aprobării înregistrării, sistemul bancar informatizat al băncii (SBI) îl înregistrează în lista celor care au drept de acces şi îi furnizează o metoda de identificare, care va fi folosită de solicitant în momentul apelării serviciului.

În general, identificarea se face prin nume şi parolă, dar pot fi şi alte metode, cum ar fi alocarea unui PBN (Personal Banking Number, util atunci când accesul la servicii se face prin mai multe canale de acces, la alegere), împreuna cu un PIN, cuplarea la calculatorul de acces la Internet a unui cititor de carduri cu cip de identificare (figura 11) sau furnizarea unui mic dispozitiv de securitate - Token (figura12), care generează un cod recunoscut de server-ul băncii, cod care e citit din dispozitiv şi introdus de solicitant. Solicitantul va plăti aceste servicii printr-un abonament lunar, în care intră diverse servicii de furnizare de informaţii la care se pot adăuga comisioane pentru unele servicii, cum ar fi plăţile.

Fig. 11. Cititor de card cu cip de identificare

Fig. 12. Dispozitive Token

Serviciile bancare electronice sunt implementate de e-bancă prin aplicații speciale aflate în SBI-ul propriu (programe, proceduri) sau, în cazul conturilor de card, în SMC-ul (Sistem de Management de Carduri) băncii. Aceste aplicații primesc solicitarea de serviciu, identifică solicitantul, efectuează serviciul cerut, trimit un mesaj de răspuns către solicitant şi păstrează o înregistrare a tranzacției. Aplicațiile de e-bancă pot fi dezvoltate chiar de bancă sau pot fi achiziționate de la furnizorii specializați. În cazul unui acces prin Internet, legăturile de telecomunicații sunt sigure (SSL - Secure Socket Layer), iar în cazul unei legături prin telefonul mobil mesajele pot fi criptate.

Efectuarea unei plăţi prin intermediul serviciului de Internet banking presupune parcurgerea următorilor paşi.:

Pasul 1. Se accesează pagina de Internet a băncii şi se apasă butonul de acces la Internet, în cazul nostru, butonul „*24 Banking*” (figura 13).

Fig. 13. Pagina de Internet a băncii

Pasul 2. Se introduce numărul de utilizator primit de la bancă în fereastra „Nume utilizator”. Se porneşte dispozitivul Token se introduce parola de accesare a dispozitivului şi se apasă tasta de generare a codului de acces (codul OTP). Acesta se introduce în fereastra „Parola” şi se apasă „Login” (figura14).

Codurile de acces ale dispozitivul Token sunt generate pe baza unui algoritm numit **one-time password** (OTP). Codul OTP are rolul unei parole ce este validă numai pentru o conectare sau numai pentru a valida o tranzacţie.

Algoritmul de generare al codului OTP se bazează pe caracterul aleatoriu al generării numerelor. Acest algoritm este necesar, deoarece altfel ar fi uşor de prezice viitoarele coduri OTP prin simpla observare a celor generate deja. Modul concret de generare a codurilor OTP diferă foarte mult în ceea ce priveşte detaliile algoritmului. Există mai multe modalităţii de generare:

– Algoritmi de generare bazate pe sincronizarea temporală dintre serverul de autentificare şi clientul ce furnizează parola (codul OTP este valid pentru o scurtă perioadă de timp – de ordinul a 30-60 secunde)

– Algoritmi de generare ce folosesc vechea parola pentru a genera o nouă parolă (codurile OTP sunt efectiv şiruri de numere ce trebuie utilizate într-o ordine predefinită)

– Algoritmi de generare la care noua parolă se bazează pe o parolă (ce poate fi un număr aleatoriu ales de serverul de autentificare sau un detaliu numeric al tranzacţiei) şi/sau un număr generat de un contor.

Fig. 14. Interfaţa de introducere a numărului de utilizator şi a codului OTP

Figura 15. Fereastra de afişare a conturilor utilizatorului

Trebuie menționat faptul că sunt disponibile diferite metode de a comunica utilizatorului noul cod OTP. Unele sisteme folosesc un dispozitiv token aflat în posesia utilizatorului ce generează codul OTP afişându-l pe un mic ecran (exemplul de față). Alte sisteme folosesc un software ce rulează pe telefonul mobil al clientului. Există şi sisteme la care serverul generează codul OTP transmițându-l clientului pe un canal sigur cum ar fi SMS-ul. În sfârşit, unele sisteme folosesc coduri OTP tipărite pe hârtie, lista aflându-se la client.

Pasul 3. Se obține o fereastră cu lista de conturi curente a posesorului (figura 15). Pentru a efectua o plată, se apasă pentru contul dorit, butonul „*Ordin de plată*” existent în dreapta. Apare fereastra prezentată în figura 16.

Fig.16. Fereastra pentru selectarea tipului de ordin de plată

Pasul 4. Se apasă butonul „*Mai mult*” din dreptul tipului de plată dorit. Se obține fereastra din figura 17. Există trei posibilități:

– În cazul unei plăți ocazionale, se introduce IBAN-ul beneficiarului în fereastra cu acelaşi nume. Se apasă butonul „Verificare IBAN”, iar dacă acesta este corect se poate efectua plata.

– În cazul plăților efectuate către furnizori de utilități (de exemplu, GDF Suez, Vodafone, Cosmote, Apa Nova etc.) se alege opțiunea „Şablon furnizor” şi se efectuează plata.

– În cazul plăților repetate efectuate către firme sau către persoane fizice care nu au un şablon predefinit, utilizatorul poate utilizeze propriile-i şabloane create în prealabil.

Fig. 17. Fereastra de creare a ordinului de plată

Pasul 5. Se alege introduce IBAN-ul beneficiarului sau se alege şablonul de plată dorit. În exemplul nostru este vorba de un furnizor de utilităţi.

Fig. 18. Selectarea şablonului pentru ordinul de plată

Pasul 6. Se introduc detaliile plății, suma şi data executării ordinului de plată (dacă este diferită de data curentă); dacă datele introduse sunt corecte se apasă butonul „*Semnează*”.

Fig. 19. Exemplu de completare a ordinului de plată electronic

Pasul 7. Se introduc cu ajutorul tastelor numerice ale dispozitivului Token, valoarea sumei şi ulterior ultimele 4 cifre ale codului IBAN, afişate cu caractere aldine (figura 20).

Fig. 20. Valorile ce trebuie introduse în dispozitivul Token

Dispozitivul va genera un cod OTP calculat pe baza unui algoritm ce ține cont de parametrii menționați anterior (suma şi ultimele cifre ale codului IBAN) şi de ora curentă. Acest cod OTP afişat pe ecranul dispozitivului Token are rol de semnătură electronică şi certifică din punct de vedere legal că ordinul de plată este emis de persoana autorizată. În exemplul nostru codul OTP este 440125.

Pasul 8. Dacă se constată o eroare în completarea ordinului de plată, acesta poate fi corectat prin apăsarea butonului „*Corectează*”. În cazul completării corecte se introduce codul OTP 440 125 în fereastra din dreptul mesajului „*Vă rugăm introduceți codul Token*” şi se apasă butonul „*Continuă*” (figura 21). Codul OTP generat de dispozitivul Token este în acest caz valabil timp de 30 de secunde. Deci din momentul afişării codului OTP până în momentul apăsării butonului „*Continuă*” nu trebuie să treacă un interval de timp mai mare de 30 secunde.

Fig. 21. Exemplu de introducere a codului OTP generat de dispozitivul Token

Odată apăsat butonul „*Continuă*” ordinul de plată este transmis către bancă iar dacă serverul de autentificare al băncii îl recunoaşte şi îl acceptă este afişat mesajul „*Ordinul de plată a fost trimis*” (figura 22).

Fig. 22. Fereastra de confirmare a acceptării ordinului de plată de către bancă

Sisteme de plată cu numerar electronic. Numerarul electronic este o noțiune nouă pentru plățile on-line deoarece combină confortul oferit de tehnica de calcul cu securitatea şi confidențialitatea oferită de numerarul fizic. Tranzacțiile prin această modalitate electronică de plată se realizează astfel: clientul cumpără numerar electronic de la furnizorul de servicii financiare prin intermediul băncilor partenere. Această operație se poate realiza atât la ghişeu prin depunerea unei sume de bani în contul furnizorului de servicii financiare cât şi on-line prin transfer între conturi.

Furnizorul de servicii financiare transferă numerarul digital către beneficiarul plății. Cererea de efectuare a plății poate fi realizată de pe calculatorul personal sau telefonul mobil. Beneficiarul plății cere furnizorului de servicii financiare să-i transfere suma în contul său bancar.

Numerarul digital poate fi folosit pentru efectuarea de plăți către comercianți şi persoane fizice, dar poate fi şi retras de către posesorul său şi transformat înapoi în numerar fizic.

Principalele caracteristici ale acestui mod de plată sunt:

- Oferă un grad ridicat de anonimat
- Necesită o infrastructură hardware rezistentă la atacuri cu scop fraudulos
- Necesită capacități de stocare ridicate
- Permite efectuarea off-line a unor operații
- Nu este necesară posesia unui card bancar

Structura numerarului electronic poate fi definită ca fiind un şir de biți ce reprezintă anumite informații precum numărul de referință şi semnătura digitală, ce pot fi utilizate cu scopul de a împiedica fraudele. Structura inițială propusă de Wright necesită extinderea sa în vederea creşterii siguranței. De aceea modelul actual prezentat în figura 23 adaugă la structura existentă o inscripție digitală similară filigranului de pe bancnote.

Valuta	Suma	Referința	Semnătura digitală	Inscripția digitală

Fig.23. Structura numerarului digital

După cum se poate vedea şirul de date conține următoarele informații:

- **Valuta numerarului digital**. Acest câmp este necesar pentru ca numerarul digital să poată opera cu mai multe valute.
- **Suma transmisă**.
- **Referința** este un număr ce permite emitentului sau oricărei părți autorizate să urmărească deplasarea numerarului digital. Este format din următoarele 4 componente:
  - Componenta emitentului, folosită ca referință de către acesta.
  - Componenta clientului ce este folosit ca referință pentru clientul ce comandă numerarul digital pentru prima dată.
  - Componenta destinatarului, folosită pentru identificarea noului proprietar al numerarului digital
  - Componenta finală folosită pentru verificarea digitului de control generat de fiecare dată.
- **Semnătura digitală** folosită pentru a autentifica identitatea emitentului ca parte autorizată.

– **Inscripția digitală** are scop protejarea dreptului de proprietate asupra numerarului digital. Aceasta inserează în şirul de informații, date invizibile pentru persoanele neautorizate.

7.3. E-frauda – principala amenințare în cazul plăților online

În prezent, frauda realizată pe Internet este la fel de diversă ca informațiile difuzate prin intermediul acestei tehnologii. Întinderea Web-ului este formată din peste 500 de miliarde de documente provenite din bazele de date conectate la Internet, fiind înregistrați mai mult de jumătate de miliard de utilizatori Internet pe plan mondial. În această vastitate de informații şi utilizatori, comerțul electronic reuşeste nu doar să ofere utilizatorilor posibilități de alegere infinite, cât şi perspective de câştig rapid prin scheme frauduloase reale cărora mediul virtual le permite propagarea. Astfel, comerțul electronic poate deveni o „oportunitate" şi în sens negativ, un instrument generator de fraude în condițiile în care, pe plan mondial, criminalitatea informatică a adus mai multe venituri decât traficul de droguri.

Există numeroase tipuri de fraude pe Internet, pornind de la simpla interacțiune dintre un vânzător şi un cumpărător în timpul unei licitații electronice, până la vizarea unui grup mai mare de victime în acelaşi timp[5]. Licitațiile frauduloase (utilizatorii intră pe site-uri precum eBay, Bid, YahooAuction, unde actul de vânzare-cumpărare se desfăşoară sub forma unei licitații, iar falsul vânzător oferă produse inexistente, deşi cel care cîştigă licitația trimite banii pentru produsul respectiv) reprezintă unul dintre cel mai frecvent tip de infracțiune în mediul online, urmată de nelivrarea de bunuri sau servicii oferite prin Internet (sau reversul: se trimit bunurile, dar nu se primesc banii), facilitată de anonimitatea relativă dată de Internet. Furtul de identitate (phising-ul) este o altă metodă de fraudare ce constă în folosirea ilegală a datelor unei persoane pentru a obține bani, a cumpăra bunuri sau a înşela. Frauda legată de investiții în afaceri inexistente este, de asemenea, o procedură ilegală întîlnită în mediul de afaceri virtual (numeroasele e-mail-urile care conțin astfel de oferte solicită fie investiții de sume relativ mici de bani în

---

[5]****Fraudele pe Internet* – Asociația pentru Protecția Consumatorilor din România - http://www.apc-romania.ro;

perspectiva, falsă, a unor sume foarte mari, fie utilizarea PC-ului penru a cîştiga facil sume importante, sau chiar oferă posibilitatea transferului unor bani în conturile potențialei victimei – cum este cazul bine cunoscut al scrisorilor electronice provenite de la persoane ce se recomandă a fi din Nigeria). Însă, folosirea frauduloasă a cărții de credit este cea mai răspândită metodă prin care se obțin ilegal numerele cărților de credit pentru ca apoi să fie folosite în mod abuziv pentru a se achiziționa produse şi servicii prin Internet, victime fiind atât posesorul cardului, cât şi vânzătorul bunului şi emitentul cardului.

Există *trei tipuri principale de fraude* mai des întâlnite în aplicațiile bazate pe *tranzacții electronice.* Primul tip este acela în care o anumită entitate pretinde că vinde ceva ce nu deține cu adevărat, dar pentru care solicită plata în avans. Un al doilea tip conduce la livrarea de bunuri sau servicii care sunt în realitate de o calitate inferioară celei pentru care s-a plătit. Un al treilea tip de fraudă se manifestă prin acțiuni de convingere a clienților să achiziționeze ceva ce ei nu doresc cu adevărat, prin intermediul unor tehnici de marketing şi de promovare foarte agresive.

O altă grupare/clasificare a fraudelor este cea legata de *sistemele de plată*, astfel:

a) Fraude care implică sisteme de plăți bazate pe hârtie: Atunci când bunuri şi servicii sunt obținute efectiv on-line, dar totuşi sunt plătite utilizând instrumente de plată bazate pe hârtie (cum ar fi ordine de plată, cecuri ş.a.), fraudele se pot realiza la fel ca în trecut. Vulnerabilitățile sunt legate în principal de utilizatori individuali ce folosesc conturi deschise folosind detalii de identificare false, de situații de depăşire a balanței creditului sau chiar de falsificarea sau alterarea unor instrumente de plată ca atare. În condițiile în care este o presiune pentru efectuarea cât mai rapidă a tranzacțiilor electronice, vânzătorii ar putea dori să nu mai aştepte ca informațiile introduse să fie şterse sau să se efectueze verificări de autenticitate înainte de autorizarea distribuirii de bunuri sau furnizării de servicii, prin urmare deschizând calea unor potențiale fraude. La rândul lor, clienții ar putea trimite informații specifice unui cec unui vânzător despre care nu dețin informații independente, care poate fi localizat într-o țară străină.

b) Fraude implicând sisteme de debit direct: Plățile on-line se pot efectua prin debit direct, caz în care sumele de bani sunt transferate direct din contul plătitorului la banca destinație sau prin intermediul unui instrument de transfer în care un client poate

solicita băncii sale să debiteze din contul său o sumă care este electronic creditată pentru alt cont. Pentru ca astfel de tranzacții să aibă loc, anumiți pași preliminari trebuie efectuați de către părțile implicate, incluzând schimbul de detalii despre conturi și realizarea a diverse verificări de identificare. Din punctul de vedere al cumpărătorului, un element de risc apare dacă fondurile sunt transferate înainte ca bunurile să sosească sau ca serviciul să fie efectiv furnizat. Din punctul de vedere al vânzătorului, este necesar ca fondurile să sosească înainte ca bunurile să fie livrate sau ca serviciul să fie furnizat. Principalul mijloc de protecție împotriva unor astfel de fraude solicită comercianților să adopte pași adecvați pentru autentificarea detaliilor de cont furnizate de către cumpărător și să se asigure că fondurile corespunzătoare sunt ținute în cont pentru a acoperi operația de cumpărare. Obținerea autorizației de la o instituție financiară este primul pas în prevenirea fraudelor.

c) Fraude implicând sisteme electronice de transfer de fonduri: Au fost dezvoltate diverse sisteme pentru a permite clienților, băncilor și comercianților să comunice în mod securizat unul cu celălalt. Respectivele sisteme electronice de transfer de fonduri au devenit deja operaționale ca substitute pentru tranzacțiile prin cecuri bazate pe hârtie, și aceste sisteme pot fi adaptate pentru utilizarea în tranzacții realizate prin Internet. Totuși, aceste sisteme creează un serios risc de securitate dacă nu se implementează proceduri adecvate pentru verificarea disponibilității fondurilor care ar trebui transferate sau pentru un control riguros al accesului la conturi. În plus, există posibilitatea manipulării și interceptării informațiilor transmise prin rețea „în clar” (în formă necriptată). De aceea, pentru a securiza operațiunile de transferuri electronice de fonduri, datele sunt de regulă criptate folosind algoritmi care codează mesajele transmise. La destinația legitimă ele vor fi decodate folosind chei cunoscute doar de către transmițător și receptor. Riscul major asociat cu un astfel de sistem constă în posibilitatea ca respectivele chei de criptare să fie interceptate, în care caz datele din cadrul sistemului ar putea fi dezvăluite sau manipulate. Majoritatea fraudelor pe scară largă la transferurile electronice de fonduri au implicat interceptarea sau alterarea mesajelor electronice transmise de la calculatoarele instituțiilor financiare. Pentru a îmbunătăți securitatea tranzacțiilor bazate pe cărți de credit și realizate prinInternet, diferite companii au proiectat sisteme care să asigure că identitatea părților contractante poate fi autentificată

şi că vânzătorii sunt capabili să determine dacă un client deține în mod real fondurile necesare pentru a putea realiza tranzacția. Microsoft şi Visa, de exemplu, au dezvoltat un protocol pentru plăți electronice numit SET (Secure Electronic Transactions) care foloseşte criptarea cu chei publice pentru a proteja datele împotriva tentativelor de compromitere sau corupere a acestora. Semnăturile digitale sunt folosite, de asemenea, pentru a autentifica fiecare dintre părțile implicate. Informațiile despre conturi sunt criptate înainte de transmisie, cheile de decriptare fiind protejate în mod separat. Principalele riscuri de securitate asociate cu aceste sisteme sunt legate de posibilitatea ca aceste chei private de criptare să fie furate sau utilizate fără autorizație de către persoane care le-au obținut în mod nelegitim. Cel mai uşor mod de a se realiza acest lucru ar fi transmiterea unei false dovezi de identificare către Autoritățile de Înregistrare atunci când se obține o pereche cheie public-privată.

d) Fraude implicând sisteme bazate pe carduri: În prezent, plățile efectuate folosind smart carduri pot lua o varietate de forme. Însă există şi riscuri aferente acestora. Principalul risc de securitate asociat cu smart cardurile este determinat de modul în care datele sunt criptate. Mecanismul de criptare utilizat poate fi spart dacă anumite tipuri de erori au apărut la nivelul cardului. Unele defecte de proiectare sau din fabricație pot spori riscurile de spargere a mecanismelor de protecție prin criptare.

e) Fraude implicând „cash" electronic (şi tranzacțiile bazate pe portofel electronic): Sunt în curs de dezvoltare variate sisteme care vor permite efectuarea de tranzacții în mod securizat prin Internet folosind „cash" electronic, sau elemente de valoare care sunt înregistrate digital pe calculatoare. Ele trebuie să folosească mecanisme de criptare eficiente, şi de regulă se bazează pe criptarea cu chei publice.

f) Fraude legate de identitate: Progresele în comerțul electronic au creat premize pentru noi forme de acțiuni ilegale şi frauduloase, puțin probabil să fie întâlnite în sistemele tranzacționale tradiționale. Spre exemplu, mulți consumatori întâmpină mari dificultăți în a-şi identifica partenerii de afaceri (sau de tranzacții realizate prin Internet). Unii comercianți recurg în mod intenționat la mascarea (ascunderea) identităților lor reale tocmai pentru a preveni posibilele fraude în tranzacțiile electronice. În practică, tehnologiile Internet asigură utilizatorilor instrumente relativ simple pentru mascarea (ascunderea) identităților reale ale acestora. Adresele de Internet, de poştă electronică,

spre exemplu, pot fi uşor manipulate pentru a include detalii care nu sunt reale, sau sursa mesajului poate fi făcută anonimă sau modificată astfel încât mesajul să apară ca provenind de la un alt utilizator.

E-frauda, în principalele sale forme de manifestare prezentate anterior, este un fenomen care se resimte şi în România. În acest sens, imaginea României în industria comerţului electronic mondial nu este una de invidiat. Studii realizate de FBI arată că am ocupat constant locuri „fruntaşe" în rândul ţărilor care generează criminalitate informatică. Românii sunt recunoscuţi în continuare în străinătate pentru fraudele de încredere, realizate mai ales pe site-urile de licitaţii online. De asemenea, în cele mai multe cazuri, activităţile infracţionale sunt iniţiate din România, dar vizează victime din străinatate sau sunt finalizate în străinatate. Autorii folosesc în comiterea acestor fapte sisteme de plată rapide oferite prin Internet (sistem escrow, conturi de PayPal, conturi e-gold, conturi de Internet-banking) sau sisteme de transfer rapid de bani (wire transfer – servicii oferite de diferite instituţii financiare). Se remarcă o tendinţă de specializare continuă a infractorilor atât asupra activităţilor desfăşurate, cât şi din punct de vedere tehnic, pentru identificarea de noi moduri de operare: licitaţii frauduloase, folosire de site-uri false de escrow, site-uri de transport, site-uri de comerţ electronic, site-uri de phishing, ascunderea urmelor prin Internet şi a circuitului produsului financiar[6]. În ceea ce priveşte criminalitatea informatică şi fraudele cu mijloace de plată, se remarcă o reorientare a grupurilor criminale, în sensul că acestea urmăresc, prin activitatea infracţionala desfăşurată, obţinerea de sume de bani importante. Din cazuistica Poliţiei Române reiese faptul că o parte din reţelele criminale organizate, transnaţionale, care în trecut îşi desfăşurau activitatea în alte domenii (trafic de autoturisme furate, trafic de fiinţe umane şi chiar trafic de droguri) s-au reorientat, săvârşind infracţiuni cu cărţi de credit şi prin Internet, sumele de bani obţinute în mod ilicit ca urmare a acestor activităţi fiind uneori mult mai mari decât cele obţinute anterior. Datele Poliţiei Române arată că jumătate din infracţiunile informatice înregistrate sunt fraude cu mijloace de plată electronice. În acest context, deşi valoarea comerţului electronic în România creşte exponenţial, românii rămân reticenţi faţă de mijloacele de plată online. Se previzionează,

---

[6] **Albăstroiu (Mărunţelu) Irina -** *Self-regulation of the e-Commerce in Romania – possible solution for the limitation of e-frauds*, Amfiteatru Economic, vol.10, nr.23, 2008, pp.142 -148;

totuşi, o tendinţă de creştere a ponderii plăţilor online, pe fondul creşterii încrederii în acest sistem de plată. Reticenţa de până acum a românilor faţă de plăţile online este pusă de specialişti pe seama neîncrederii în siguranţa tranzacţiilor pe Internet, pe cea a tradiţiei plăţilor cash, dar şi pe cea a lipsei obişnuinţei de cumpărare pe Internet. De asemenea, aceştia consideră că aceste bariere pot fi depăşite prin lărgirea accesului populaţiei la tehnologiile informaţionale şi prin trecerea online a unor servicii ale administraţiei publice (de exemplu, plata amenzilor, a taxelor şi impozitelor), lucruri care i-ar familiariza pe români cu procedurile comerţului electronic.

În aplicaţiile de e-commerce, fraudele apar ca rezultat a trei factori: existenţa unor infractori motivaţi, disponibilitatea unor ţinte accesibile şi absenţa unor măsuri de protecţie adecvate. Creşterea numărului de entităţi implicate în tranzacţii specifice aplicaţiilor de comerţ electronic a condus la sporirea disponibilităţii pentru tot mai multe ţinte probabile ale infractorilor cibernetici. Majoritatea tranzacţiilor electronice presupun şi vehicularea unor multiple tipuri de informaţii colaterale despre părţile implicate, informaţii care pot fi uşor interceptate de către atacatori din Internet. În plus, viteza cu care tranzacţiile on-line se desfăşoară facilitează şi fraudele, deoarece în multe cazuri părţile implicate în tranzacţii nu dispun de timpul necesar pentru a reflecta asupra condiţiilor şi termenilor propuşi în cadrul respectivelor tranzacţii comerciale prin Internet. Aceştia nu pot verifica nici identitatea reală a presupuşilor parteneri, ceea ce constituie o altă vulnerabilitate şi o premiză pentru acţiuni frauduloase. Unele metode de control implementate la nivel organizaţional pentru a preveni fraudele nu se pot totuşi aplica pentru tranzacţiile on-line (realizate prin Internet), în care acordurile trebuie încheiate rapid, iar plăţile trebuie efectuate cvasi-instantaneu (prin transferuri de fonduri prin mijloace electronice). Tehnologiile suport pentru sistemele de e-commerce asigură multiple posibilităţi şi pentru cei care doresc să obţină foloase necuvenite prin acţiuni frauduloase asupra sistemelor informatice şi de comunicaţii care susţin aplicaţiile de comerţ electronic. Prin urmare, elaborarea unor strategii eficiente de management al fraudelor, de prevenire şi limitare a efectelor acestora, este o prioritate pentru organizaţiile implicate în realizarea de tranzacţii electronice pentru aplicaţii de e-commerce.

Fiabilitatea, *autenticitatea*, *integritatea* şi *utilizabilitatea* sunt caracteristicile

utilizate pentru a descrie nivelul de încredere în informațiile transmise în cadrul unor aplicații cum ar fi cele de e-commerce.

Fiabilitatea: O înregistrare fiabilă este una al cărei conținut poate fi de încredere ca o reprezentare completă şi precisă a tranzacțiilor, activităților sau faptelor pe care acestea le desemnează.

Autenticitatea: O înregistrare autentică este una dovedită a fi ceea ce se presupune a fi şi care a fost creată sau transmisă de persoana presupusă de la început ca fiind la originea respectivei înregistrări. Pentru a demonstra autenticitatea înregistrărilor, este necesar să se implementeze şi să se documenteze politici şi proceduri care să controleze crearea, transmiterea, primirea şi întreținerea înregistrărilor de date, pentru a verifica faptul că autorii înregistrărilor sunt autorizați şi identificați şi, de asemenea, pentru a asigura că înregistrările sunt protejate împotriva accesărilor neautorizate.

Integritatea: Integritatea unei înregistrări se referă la faptul că aceasta trebuie să rămână completă şi nemodificată. Este necesar ca o înregistrare să fie protejată împotriva încercărilor neautorizate de modificare (din partea unor entități care nu dețin permisiuni în acest sens). Un alt aspect se referă la integritatea structurală a înregistrării. Structura unei înregistrări (deci formatul său fizic şi logic, precum şi relațiile dintre elementele de date conținute) ar trebui să rămână, de asemenea, intactă fizic şi logic.

Utilizabilitatea: O înregistrare utilizabilă este una care poate fi localizată, regăsită, prezentată şi interpretată. Pe parcursul oricărei încercări ulterioare de regăsire şi utilizare, înregistrarea trebuie să poată fi accesată şi utilizată în orice tranzacție din cadrul unor aplicații cum sunt cele de e-commerce, e-health, egovernment, e-learning şi e-work.

Politici adecvate de control şi management al fraudelor trebuie adoptate pe scară largă atât în sectorul public, cât şi în cel privat. Din perspectivă tehnologică, o gamă largă de soluții au fost proiectate şi introduse în scopul reducerii riscurilor de fraude electronice pentru tranzacțiile comerciale realizate prin Internet (în aplicații de comerț electronic).

În ceea ce priveşte *securitatea echipamentelor (hardware*), acestea trebuie protejate astfel încât să se restricționeze accesul la resursele informaționale stocate, eventual prin firewall sau alte dispozitive, în scopul prevenirii unor intruziuni capabile să conducă la fraude electronice cu consecințe serioase pentru instituțiile financiare sau firmele implicate.

Autentificarea utilizatorilor trebuie implementată astfel încât să reducă la minim riscul fraudelor legate de identitate (prin furt de identitate, mascarea identității, etc.). Cât timp procedurile de autentificare sunt ineficiente, atacatorii pot evita responsabilitatea pentru acțiunile lor, iar probabilitatea unor fraude în sistemele de comerț electronic rămâne ridicată. În principiu, metodele de identificare/autentificare folosite în sistemele actuale de e-commerce sunt de 3 tipuri principale: sisteme de identificare bazate pe cunoştințe, metode de autentificare biometrice şi metode bazate pe „jetoane" („token"-uri). Sistemele de identificare bazate pe cunoştințe sunt predispuse la multiple riscuri şi trebuie serios protejate. Cum majoritatea sistemelor de plată online necesită utilizarea unor PIN-uri (Personal Identification Number) sau parole pentru ca utilizatorii să obține accesul la resursele informatice, protecția acestor date de acces reprezintă prima şi cea mai evidentă strategie de prevenire a fraudelor. Parolele sunt adesea utilizate în mod inadecvat şi pot fi ghicite cu uşurință, mai ales dacă nu au fost alese cu atenție, respectând anumite reguli în măsură să reducă probabilitatea de a fi ghicite. Unele sisteme impun, ca măsură suplimentară de protecție, schimbarea periodică a parolelor, sau chiar utilizarea unor parole de singură folosință, în sensul că la următoarea utilizare a sistemului se generează o nouă parolă pentru realizarea tranzacției comerciale prin Internet, parolă diferită de cea utilizată în cadrul sesiunii precedente. Metodele de autentificare biometrică devin de un interes sporit deoarece aparent ele oferă un nivel de integritate mai ridicat, în comparație cu sistemele de identificare bazate pe cunoştințe şi cu cele bazate pe jetoane (dispozitive dedicate pentru controlul accesului). Se preconizează ca în viitor tehnologiile de autentificare bazate pe metode biometrice să asigure un nivel mai ridicat de securitate, deşi problemele de confidențialitate şi de protecție a caracterului privat vor continua să rămână în atenție. Deja există o varietate de sisteme care exploatează particularități fizice proprii ale indivizilor pentru a realiza o autentificare mai sigură. Identificatorii biometrici comuni în prezent includ amprentele degetelor, patern-uri vocale, patern-uri de tastare, imagini retiniene, caracteristici faciale. De exemplu, sistemele de identificare bazate pe amprente sunt utilizate pentru a restricționa accesul la tastaturi sau atunci când se foloseşte un mouse. Un dezavantaj este acela că deşi astfel de sisteme oferă nivele de securitate mai ridicate decât cele realizate de sistemele bazate pe parolă, ele sunt încă destul de costisitoare pentru a fi utilizate pe o scară largă. În plus, se

ridică problema confidențialității şi a protecției caracterului privat al informațiilor personale stocate în rețelele de calculatoare.

În ceea ce priveşte securitatea *sistemelor bazate pe semnătură digitală*, trebuie remarcat faptul că sistemele de criptare cu chei publice reprezintă una dintre cele mai eficiente abordări pentru a permite realizarea în condiții mai sigure a tranzacțiilor de comerț electronic prin Internet. Fraudele în aplicațiile de comerț electronic trebuie prevenite sau, dacă tot au apărut, trebuie să fie detectate rapid pentru a li se limita pe cât posibil consecințele. Dacă nu este posibil să se prevină 100% acțiunile frauduloase on-line, cel puțin poate fi posibil ca prin intermediul unor soluții software de detecție să se identifice prezența unor acțiuni tranzacționale frauduloase, şi aceasta tocmai pentru a reduce potențialele pierderi cauzate de astfel de fraude. Diferite firme dezvoltă soluții software dedicate utilizate în prevenirea fraudelor electronice. O altă modalitate în care fraudele pot fi detectate se bazează pe monitorizarea activității pe Internet a angajaților companiilor. Utilizarea sistemelor de calcul de către angajați, şi mai ales activitățile online ale acestora, pot fi monitorizate prin soluții software care țin evidența pentru respectivele activități. De asemenea, filtrarea accesului către exterior (prin politici adecvate la nivel de firewall, de exemplu) poate preveni sau limita tentativele de fraudă prin Internet.