FRAUDE PRIN INTERMEDIUL CARDURILOR BANCARE

Ion CIOBANU*[*], *Georgeta GHERGHINA*[**], *Alexandru GRIBINCEA

[*]*InvestPrivatBank, Chişinău*
[**]*Agenţia Raiffeisen Bank SA, Constanţa*
Catedra Marketing şi Relaţii Economice Internaţionale

Today may be noting an interdependency manifest between the process of migrating to chip and technology the fraud through credit cards. In the Europe and Asia Pacific, which is always recording high rates of fraud with bank cards, the migration to EMV technology started in 2006. Thus, according to statistical data provided by MasterCard in Europe have migrated to chip 35% of the total number of cards, and 15% in Asia Pacific region. However, rates of migration to chip technology in the U.S. and Australia are much lower, the explanation being reduced crime with credit cards in these countries.

Astăzi poate fi remarcată o interdependenţă vădită între procesul de migrare către tehnologia cip şi nivelul fraudelor, prin intermediul cardurilor bancare. În regiunea Europa şi Asia Pacific, unde întotdeauna se înregistrau ritmuri înalte de fraude cu cardurile bancare, procesul de migrare către tehnologia *EMV*[*] a demarat în 2006. Astfel, conform datelor statistice oferite de MasterCard, în Europa au migrat către cip 35% din numărul total al cardurilor şi, respectiv, 15% în regiunea Asia Pacific.

Totodată, ritmurile de migrare către tehnologia cip în SUA şi Australia sunt mult mai reduse, explicaţia fiind rata redusă a infracţiunilor cu carduri bancare în aceste ţări.

De asemenea, este de menţionat că pentru regiunea SUA încă nu au fost stabilite termene exacte privind intrarea în acţiune a principiului „transferului de responsabilitate" (Chip liability shift)[**], conform căruia responsabilitatea deplină revine părţii care la momentul identificării situaţiei-problemă nu a implementat tehnologia EMV (Europay, MasterCard şi Visa).

Conform estimărilor, în anul 2004 pierderile băncilor din Marea Britanie, ca urmare a fraudelor cu cardurile bancare, au depăşit 0,5 miliarde lire sterline. Conform aceloraşi estimări, dacă băncile continuau să utilizeze carduri cu bandă magnetică, atunci în 2005 aceste pierderi ar fi constituit de la 800 milioane până la 1 miliard lire sterline. În acest sens, Marea Britanie s-a dovedit a fi un exemplu remarcabil în ceea ce priveşte eficienţa implementării tehnologiei cip: în 2005 pierderile s-au redus cu 13% în raport cu anul 2004.

În special, pierderile generate de falsificarea cardurilor (couterfeit) s-au redus cu 25%, iar în rezultatul cardurilor pierdute/furate acest indice a arătat o reducere cu 22%. De menţionat că în Marea Britanie au fost implementate cardurile cu cip care susţin regimul off-line de verificare a PIN-codului (tehnologia Chip&PIN), ceea ce, în rezultat, a contribuit la reducerea pierderilor în urma utilizării de către infractori a cardurilor pierdute sau furate.

Astfel, trecerea continuă la tehnologia cip şi creşterea numărului de carduri cu microprocesor în circulaţie contribuie semnificativ la reducerea, la nivel de ţară, regiune, a pierderilor băncilor aferente activităţii cu carduri [1]. Totodată, sporirea eficienţei acestui proces de migrare depinde în mare parte de sincronizarea acţiunilor tuturor participanţilor, în special a sistemelor de plăţi şi a băncilor emitente, fapt ce impune tot mai evident conştientizarea de către toţi actorii implicaţi a necesităţii implementării standardelor EMV, în special în regiunea SUA, unde acest indice continuă a fi unul scăzut.

Din aceste considerente, este importantă existenţa unei instituţii unice la nivel naţional, care ar avea funcţia de coordonare şi reglare în procesul de migrare către tehnologia cip. Spre exemplu, în Marea Britanie această funcţie revine Asociaţiei Interbancare APACS, care a determinat strategia de migare a băncilor comerciale către cardurile cu microprocesor, cu metoda de verificare în regim off-line a PIN-codului. De asemenea, această instituţie a elaborat graficul de migrare şi asigură controlul asupra realizării acestui program [2].

[*] EMV – Europay, MasterCard and Visa standardul sistemelor de plăţi Europay, MasterCard şi Visa. Astfel, sistemul de procesare a cardurilor în ceea ce priveşte acceptarea şi procesarea tranzacţiilor derulate prin intermediul cardurilor cu cip.
[**] Liability shift – procesul de transmitere a responsabilităţilor.

Pentru a avea o imagine reală şi de ansamblu asupra faptului ce pericol reprezintă fraudele cu carduri pentru activitatea unei instituții bancare care a implementat proiectul EMV, este necesar de a avea o prezentare complexă despre factorii determinanți şi dinamica de dezvoltare a activității cu carduri în cadrul băncii.

Pentru estimarea nivelului fraudelor în raport cu cardurile emise în cadrul unei bănci, poate fi utilizată următoarea formulă de calcul:

a) cota-parte din tranzacțiile efectuate cu cardurile băncii în rețeaua de terminale pe teritoriul țării;

b) cota-parte din tranzacțiile efectuate cu cardurile băncii în rețeaua de terminale la nivel regional, care include banca;

c) cota-parte din tranzacțiile efectuate cu cardurile băncii în rețeaua de terminale la nivel regional, care nu include banca;

A – cota-parte de carduri cu cip a băncii corespunzătoare;

B – cota-parte de terminale care acceptă carduri cu cip, la nivelul regiunii din care nu face parte instituția bancară analizată;

f1, f2, f3 – nivelul fraudelor, reflectate în puncte de bază, care se referă, respectiv, la nivelul național, regional, interregional.

Presupunem că: instituția bancară face parte din regiunea în care acționează deja principiul transferului de responsabilitate şi banca emite carduri cu cip, care implică şi verificarea în regim off-line a PIN-codului[*]. Reieşind din această situație, obținem următoarea formulă matematică care reflectă rata fraudelor la nivelul băncii, din punctul de vedere al numărului de carduri emise:

$$F = [f1a+f2b+f3c\ \{1-B\}]\{1-A\}$$

Drept urmare, asupra nivelului fraudelor (din punctul de vedere al impactului asupra băncii emitente) influențează nu doar numărul de carduri cu cip emise, dar şi capacitatea de amplasare/răspândire a rețelei de terminale a băncii respective în alte țări şi regiuni.

Analizând Tabelul de mai jos, obținem următoarele concluzii:

Tabel

Amplasarea şi tipurile de terminale

Amplasare terminal	Rețea la nivel național		Rețea la nivel regional		Rețea extraregională	
Tip terminal / *Tip card*	EMV	Non-EMV	EMV	Non-EMV	EMV	Non-EMV
EMV	0	A	0	A	0	A
Non-EMV	I	I	I	I	I	I

Rândurile două de jos din Tabel reprezintă situații de utilizare a cardurilor fraudate, la care banda magnetică este creată în baza datelor furate de pe altă bandă magnetică, fiind vorba astfel despre un card combinat EMV şi cu bandă magnetică (non-EMV).

Coloanele indică tipul terminalului în care este utilizat (introdus) cardul fraudat. Tipul terminalului este determinat de regiunea în care acesta este amplasat şi de posibilitatea procesării de către dispozitiv a tranzacțiilor EMV.

Indicatorii reflectați în Tabel reprezintă consecințele situațiilor de utilizare a cardurilor fraudate în anumite tipuri de terminale. Sunt utilizați următorii indicatori:

I – frauda va avea loc. Responsabilitatea – emitent;

A – frauda va avea loc. Responsabilitatea – Acquirer;

0 – frauda nu este posibilă.

Notă: În cadrul acestui studiu, considerăm posibilitatea nulă de producere a fraudei, în cazul utilizării cardului fraudat de tip EMV într-un terminal EMV.

Totuși, şi în această situație pot fi excepții, şi anume:

✓ Într-un terminal EMV poate fi utilizat cu succes un card EMV pierdut/furat, dacă cardul nu susține procedura de verificare a PIN-codului în regim off-line.

[*] PIN-cod *(Personal Identification Number)* – este număr personal de identificare, cu caracter strict confidențial, atribuit de bancă deținătorului de card, care conferă titularului siguranța în efectuarea tranzacțiilor, accesarea terminalului bancar şi preîntâmpină utilizarea cardului de către alte persoane neautorizate. PIN-codul este considerat ca echivalent electronic al semnăturii titularului de card.

✓ Datele de pe banda magnetică a cardului de tip EMV pot fi citite şi înscrise pe card fraudat, indicând codul de deservire „1" şi utilizând cardul în regim „Floor limit" (în regimul dat valoarea CVC/CVV nu se verifică).

Să analizăm următorii indicatori, în cadrul unui proiect de emitere a cardurilor EMV. 40% – carduri EMV emise de bancă.

A = 0,96; b = 0,03; c = 0,01; f1 = bp; f2 = 40bp; f3 = 60bp; 7 = 0; B = 0,1.

Astfel, în rezultatul migrării la cip, nivelul fraudelor se va reduce de la 7,56 p până la 4,5 bp. Deci, dacă A=0,6, nivelul fraudelor din punctul de vedere al emiterii se va reduce până la 3,0 bp. Desigur, modelul prezentat mai sus nu ia în consideraţie multitudinea factorilor, cum ar fi, spre exemplu, migrarea la cip în regiuni cu infrastructura slab dezvoltată a procesării tranzacţiilor cu cardurile EMV. Este de menţionat că nivelul fraudelor cu cardurile bancare la nivel interregional este monitorizat continuu prin intermediul soluţiilor soft specializate utilizate de bănci.

Deoarece utilizarea tehnologiilor EMV cunoaşte niveluri diferite de dezvoltare în ţări şi regiuni, putem presupune că sistemele de plăţi cu carduri vor permite băncilor să emită atât carduri EMV, cât şi cu bandă magnetică, pentru a oferi clienţilor posibilitatea utilizării lor în regiunile care încă nu au migrat la tehnologia EMV. Această strategie poate fi utilizată reuşit în calitate de instrument suplimentar pentru reducerea nivelului de fraudă cu cardurile [3].

Modelul descris poate fi utilizat şi pentru estimarea nivelului de fraude cu carduri la nivel de ţară, în cadrul proiectelor de emitere sau acceptare.

Specificul etapei de tranziţie la EMV

Conform estimărilor Frost&Sullivan, pierderile suportate de băncile comerciale din întreaga lume în 2005 în urma fraudelor cu carduri au constituit 7,9 miliarde USD, iar către 2009 acestea ar putea atinge cifra de 15,5 miliarde USD.

Aceste cifre demonstrează abilitatea infractorilor de a se adapta rapid la noile implementări şi realizări în domeniu. Aceasta diminuează posibilităţile băncilor de a reduce nivelul fraudelor în domeniu, în special la etapa iniţială de migrare la tehnologia cip.

Pentru început, este necesar a menţiona că în următorii 10-15 ani vor continua să se efectueze tranzacţii cu carduri care dispun de bandă magnetică şi duale, la terminale care nu susţin cardurile cu cip. Acest lucru oferă infractorilor posibilitatea de a utiliza cardurile cu bandă magnetică în scopuri de fraudă, şi anume:

✓ Utilizarea datelor înscrise pe banda magnetică pentru confecţionarea unui card fraudat şi utilizarea ulterioară a acestuia la POS-terminal care nu susţine tehnologia EMV.

✓ Falsificarea cardurilor combinate (spre exemplu: personalizarea incorectă a cipului şi utilizarea procedurii de „Fallback" pentru banda magnetică, sau schimbarea codului de deservire pentru trecerea cardului spre deservire în regim „Floor Limit").

Este evident faptul că dacă cardul nu susţine regimul off-line de verificare a PIN-codului, în consecinţă cardurile pierdute/furate pot fi utilizate fraudulos în terminale (atât EMV, cât şi non-EMV). O lacună considerabilă prezintă utilizarea de către bănci a regimului „Fallback" pentru banda magnetică. Astăzi, atât sistemele internaţionale de plăţi cu carduri, cât şi băncile comerciale tind să renunţe la această modalitate, dar excluderea definitivă nu este încă pe deplin posibil a fi realizată. Spre exemplu, conform datelor MasterCard, în 2006, 18% din totalul tranzacţiilor cu cardurile cu microprocesor în terminalele cu cip din Marea Britanie erau efectuate în regim „Fallback". În medie, acest indice la nivelul întregului continent european constituie 2-4%, considerat oricum de specialişti ca fiind ridicat. Statele europene manifestă o tendinţă tot mai vădită de a renunţa la mecanismul tranzacţiilor în regim „Fallback".

Fraudele în domeniul cardurilor se intensifică în special în acele sectoare ale activităţii cu carduri ale băncilor care sunt mai vulnerabile. Din aceste considerente, segmentul tranzacţiilor de tip CNP (Card not present transactions) constituie următoarea ţintă a infractorilor în domeniul fraudelor cu cardurile bancare, deoarece cardurile cu microprocesor au contribuit deocamdată minimum la reducerea nivelului fraudelor. Minimizarea fraudelor pe segmetul tranzacţiilor de tip CNP s-a redus la utilizarea cardurilor cu cip în modelul dual de autentificare, şi anume: autentificarea cardului conform criptogramei AAC şi a deţinătorului de card, prin utilizarea PIN-codului. Această metodă de autentificare a fost denumită TBA (Token Based Authentication) – în cadrul VISA International şi Chip Authentication Program (CAP) – în cadrul MasterCard International [4].

Exemplul Marii Britanii vine să demonstreze că în cadrul procesului de migrare la tehnologia EMV fraudele de tip CNP vor deveni tot mai frecvente. Pe parcursul ultimilor trei ani, această metodă de fraudă a ocupat primul loc în rândul infracţiunilor în domeniul cardurilor bancare şi manifestă continuu un ritm sporit de creştere. Astfel, în 2005 pierderile anuale generate de fraudele de tip CNP cu cardurile bancare a constituit 21%, în valoare de 183,2 milioane lire sterline, ceea ce depăşeşte de 2 ori pierderile generate de tranzacţiile cu cardurile falsificate şi de 2 ori mai mult pierderile generate de tranzacţiile cu cardurile pierdute/furate.

Spre regret, metodele propuse spre utilizare astăzi în domeniul tranzacţiilor cu cardurile în mediul electronic nu dau efectele scontate, din cauza nivelului redus de aplicare. Nivelul fraudelor cu cardurile bancare în mediul e-commerce constituie aproximativ 20-25 puncte. Pentru lupta împotriva fraudelor pe segmentul CNP, băncile trebuie să pună accentul pe utilizarea tot mai largă a protocolului 3D Secure. Aceasta deoarece la etapa actuală acest protocol reprezintă cea mai securizată schemă de autentificare a deţinătorului de card la efectuarea tranzacţiilor cu cardurile în mediul electronic, aplicat atât în cadrul sistemului internaţional de plăţi VISA, cât şi MasterCard. De asemenea, conform regulilor stabilite de aceste sisteme internaţionale de plăţi cu carduri, doar la utilizarea acestor mecanisme – Verified by VISA şi MasterCard Secure Code – în cazul apariţiei unor situaţii de dispută, responsabilitatea revine părţii emitente. Din aceste consdirente, băncile emitente trebuie să fie cointeresate în atragerea deţinătorilor de carduri pentru utilizarea mecanismului 3D Secure.

La etapa actuală, nivelul de implementare şi aplicare a protocolului 3D Secure în mediul e-commerce este destul de ridicat, fiind utilizat de către cele mai cu renume puncte comerciale în mediul electronic. Totodată, au apărut unele impedimente la etapa atragerii deţinătorilor de carduri pentru utilizarea acestui mecanism la efectuarea tranzacţiilor. Pentru ca clientul unei bănci care aplică pe larg mecanismul 3D Secure să poată efectua tranzacţii în mediul e-commerce, sunt necesare o serie de acţiuni specifice. Astfel, deţinătorul de card trebuie să acceseze serverul special al băncii emitente (enrollment server) pentru a se înregistra în programa 3D Secure, prin care primeşte de la banca emitentă anumite date confidenţiale, cum ar fi cuvântul-parolă şi Personal Authentication Message, care, în continuare, sunt utilizate pentru autentificarea sa de către emitent, la momentul efectuării tranzacţiilor cu cardul în mediul electronic. Desigur, există o serie de posibilităţi, prin care acest mecanism este simplificat şi aproape exclude necesitatea efectuării acţiunilor sus-menţionate de către deţinătorul de card. Una dintre soluţiile, prin care deţinătorii de card sunt motivaţi de a utiliza mecanismul 3D Secure, este utilizarea mecanismului de autentificare similar celui de Internet-banking.

Aceasta demonstrează probabilitatea creşterii ratei fraudelor de tip CNP cu cardurile bancare. În ceea ce priveşte piaţa cardurilor bancare din Federaţia Rusă, este de menţionat că, conform datelor statistice oferite de Asociaţia Naţională a Participanţilor Comerţului Electronic, volumul tranzacţiilor cu cardurile în mediul e-commerce în anul 2005 a constituit 4,47 miliarde USD, înregistrând o sporire anuală cu 38%.

Ponderea tranzacţiilor în mediul electronic cu cardurile bancare în Federaţia Rusă constituie 1% din totalul cumpărăturilor efectuate în mediul virtual, ceea ce denotă indici destul de reduşi, comparativ cu întregul continent european, în Europa constituind mai mult de 10%. Conform estimărilor specialiştilor în domeniul securităţii tranzacţiilor cu cardurile bancare, odată cu sporirea gradului de securitate a cardurilor, atenţia infractorilor se va îndrepta tot mai mult spre reţeaua de acceptare şi deservire a cardurilor bancare. Este de menţionat că aceste dispozitive erau destul de vulnerabile şi anterior, dar nu prezentau interes pentru infractori, deoarece existau alte căi de fraudare a tranzacţiilor cu carduri. Deoarece terminalul este astăzi similar unui computer personal, acest fapt permite infractorilor utilizarea unor metode deja utilizate de atac, în special aşa-numitele programe virusate (spyware, Trojan horse, keyboard/screen logger), care permit infractorilor sa obţină informaţia înscrisă pe card şi utilizarea ei în scopuri criminale. De cele mai multe ori, aceste atacuri implică obţinerea PIN-codului, înscrierea în aplicaţia corespunzătoare a terminalului a cheii eronate a sistemului etc.

Pentru a exclude posibilitatea de a schimba aplicaţia terminalului, se utilizează resursele sistemului operaţional şi ale dispozitivului criptoprocesoral. De menţionat că pentru terminalele care acceptă cardurile cu cip această problemă se exclude prin utilizarea unui card special cu microprocesor, care îndeplineşte funcţiile cheii de acces la operaţiuni.

O altă problemă care necesită atenţie deosebită vizează înlocuirea de către infractori a POS-terminalului băncii cu un POS-terminal „fals”. Costul unui astfel de dispozitiv nu este prea mare şi variază de la 325 la 600 USD. Asemenea acţiuni, de regulă, au loc prin cârdăşia dintre infractori cu angajatul din cadrul punctului

comercial. Sunt cunoscute cazuri similare de instalare şi a ATM-urilor „false". De asemenea, punctul comercial poate utiliza POS-terminalul, la fel în scopuri criminale, doar pentru a colecta informaţia înscrisă pe banda magnetică a cardului.

Astfel, în cazul utilizării unui POS-terminal „fals", la introducerea cardului, are loc copierea nu doar a informaţiei înscrise pe banda magnetică, ci şi a valorii PIN-codului. Deci, chiar şi în condiţiile utilizării cardurilor combinate este suficientă doar înscrierea datelor de pe banda magnetică şi a valorii PIN-codului, pentru ca ulterior să fie confecţionate aşa-numitele „plasticuri albe" şi utilizate în scopuri criminale în ATM-uri. Pentru excluderea problemei cu utilizarea terminalului „fals", este necesară instalarea codului MAC (Message Authentication Code) la prelucrarea tranzacţiilor în regim on-line pentru schimbul de informaţii între terminal şi sistemul automatizat al băncii. Aceasta asigură integritatea procesului de schimb de informaţie şi autentificarea POS-terminalului. Totuşi, utilizarea codului de tip MAC asigură securitatea doar în cazul tranzacţiilor efectuate în regim on-line. În ceea ce priveşte informaţia despre tranzacţiile efectuate în regim off-line, aceasta, de asemenea, poate fi criptată şi transmisă către sistemul automatizat al băncii, dar în cazul utilizării terminalelor „false" această procedură poate dura destul de mult sau nu va avea loc nicicând. Din aceste considerente, în cazul efectuării tranzacţiilor în regim off-line la terminale, măsurile de securitate actualmente sunt destul de minime şi se reduc, de regulă, doar la limitarea accesului fizic la aceste dispozitive. O metodă efectivă de luptă împotriva terminalelor „false" ar fi instalarea unui mecanism de autentificare reciprocă între card şi terminal, la momentul iniţierii tranzacţiei.

În linii generale, metodele de atac asupra cipului sunt mult mai costisitoare. Printre atacurile de această natură pot fi menţionate clonarea cardurilor SDA şi a cardurilor DDA/CDA personalizate incorect pentru utilizarea cardurilor fraudate în tranzacţiile off-line, precum şi metodele atacurilor fizice asupra cardului cu cip (Single Power Attack/Differential Power Attack, Differential Fault Attack, Timing Analysis Attack. etc), care, în opinia experţilor, vor fi utilizate doar după epuizarea metodelor tradiţionale de fraudare.

Concluzii

Pe măsura extinderii infrastructurii cardurilor cu microprocesor, fraudele în acest domeniu de asemenea vor suporta schimbări – atât calitative, cât şi cantitative.

Dacă din punct de vedere cantitativ acestea se vor reduce, vor creşte, însă, costurile efectuării acestor fraude. Din punct de vedere calitativ, aceste schimbări se vor manifesta prin deplasarea fraudelor în regiunile mai puţin dezvoltate şi prin ponderea diferitelor categorii de fraude în totalul tranzacţiilor efectuate cu cardurile pierdute/furate/contrafăcute. Astfel, iniţialmente putem constata o creştere a ponderii fraudelor aferente tranzacţiilor de tip CNP, la care se vor adăuga şi atacurile tot mai vădite asupra reţelelor de terminale ale băncilor comerciale. Ulterior, putem estima tentative de atac asupra cardurilor cu cip, dar care vor fi, la prima etapă, destul de reduse ca număr şi efecte potenţiale. Din aceste considerente, la etapa implementării proiectelor EMV, băncile comerciale trebuie în continuare să atragă atenţie deosebită măsurilor de securitate şi să nu mizeze în totalitate doar pe înseşi cardurile cu cip. Este necesară modificarea sistemelor frontale, în special prin adaptarea programelor şi mecanismelor de monitorizare a tranzacţiilor efectuate cu cardurile combinate, de asemenea, în ceea ce priveşte metoda corectă de personalizare a cardurilor, securitatea tranzacţiilor cu carduri în reţeaua Internet etc. În aceste scopuri, băncilor li se recomandă să pregătească proprii specialişti în domeniul securităţii tranzacţiilor cu cardurile bancare, precum şi să apeleze la serviciile outsourcing. Desigur, implementarea cardurilor cu cip nu va rezolva definitiv problema fraudelor în domeniul respectiv, dar va contribui considerabil la reducerea numărului de infracţiuni.

Referinţe:

1. Edward A. Kolodziej. Securitatea şi relaţiile internaţionale // Le monde-diplomatique. - 2009. - Nr.37. - P.24.
2. http ://www .securizare.ro/content/view/829/38/
3. http ://www .infofirme.com/firme_272-sisteme+de+securitate+bancara.html
4. http ://www .arb.ro/comisie.php?id=4&c=Comisia-de-securitate-bancar%C4%83

Prezentat la 02.07.2009