MINISTERUL EDUCAŢIEI NAŢIONALE
UNIVERSITATEA „VALAHIA” din TÂRGOVIŞTE - IOSUD
Str. Lt. Stancu Ion, Nr. 35 – 130105, Târgovişte, România
Tel/Fax: +40-245-206104
http://scoaladoctorala.valahia.ro/

TEZĂ DE DOCTORAT:

Dezvoltarea resurselor umane în vederea optimizării securității plăților online

CONDUCĂTOR DE DOCTORAT:
Prof.univ.dr. Mohammad JARADAT

DOCTORAND:
Marius BURCĂ

TÂRGOVIŞTE
2018

CUPRINS

CUVINTE CHEIE

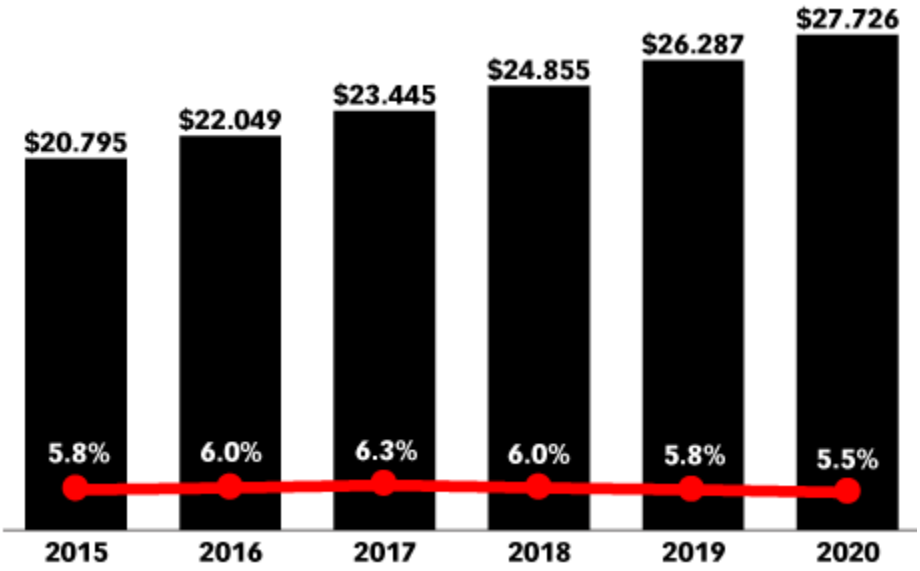
Plăți online
Dezvoltarea resurselor umane
Anti-fraudă
Spălare de bani
Managementul riscului plăților online
Comportamentul organizațional
Jocuri de noroc
Analiza comportamentală
Infracționalitatea gulerelor albe

SINTEZA TEZEI DE DOCTORAT

Odată cu globalizarea și apariția Internetului, comerțul electronic continuă să se dezvolte și să ocupe un rol din ce în ce mai important în viețile noastre. Volumul tranzacțiilor în 2016, la nivel mondial, s-a situat la valoarea de 22,049 mii de miliarde de dolari, în creștere cu 6% față de anul 2015, conform unui studiu de specialitate[1].

Același studiu prognozează că nivelul anual de creștere se va menține până în anul 2020:

Figura 1 – Evoluția comerțului electronic la nivel mondial



(Sursa eMarketer[2])

Și în România comerțul electronic este în continuă creștere. Un studiu al GpeC[3] arată că în anul 2016 volumul cumpărăturilor online au urcat la valoarea de 1,8 miliarde de euro, în creștere cu 30% față de anul 2015. Același studiu estimează că în țara noastră sunt 11,2 milioane de utilizatori de internet, asigurând o rată de penetrare de 58% din totalul populației.

---

[1] Emarketer (22 aug 2016), „Worldwide Retail Ecommerce Sales Will Reach $1.915 Trillion This Year", disponibil online la https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369 și accesat la 21.08.2017, orele 17:32

[2] Emarketer (22 aug 2016) opus citatum

[3] Blogul GPec (17 ian 2017) disponibil online la http://www.gpec.ro/blog/bilantul-pietei-de-e-commerce-2016-romanii-au-cumparat-online-de-peste-18-miliarde-de-euro-infografic și accesat la 22.08.2017, orele 10:42

Din cei 11,2 milioane de utilizatori de internet, 6,7 milioane au făcut cel puțin o dată cumpărături online în 2016, iar 2,34 milioane au folosit un dispozitiv mobil (telefon, tabletă).

Cu toate acestea, din totalul cumpărăturilor online, doar 6% au fost efectuate cu cardul bancar, deși sunt emise circa 14,5 milioane de carduri. De altfel, 90% din plățile online s-au realizat prin ramburs, în numerar, la livrarea produsului, iar restul de 4% prin alte metode (online banking, micro-plăți prin SMS etc.).

Tabelul 1 – Structura metodelor de plată în comerțul electronic din România în 2015

Metoda de plată	**Procentul din total tranzacții**
Ramburs la livrare	90,00%
Plata online cu cardul bancar	6,00%
Alte metode (online banking, SMS, eWallet)	4,00%

(Sursa GPeC[4])

De aici reiese reticența utilizatorilor de carduri bancare în a le folosi pentru plăți online, și pe bună dreptate: plățile online cu cardul prezintă riscuri.

În acest context, pentru a putea ține pasul cu evoluția comerțului electronic, toate entitățile implicate în plățile online (atât comercianții, cât și prestatorii de servicii de procesare a plăților online) trebuie să asigure suficiente metode de prevenire și combatere a infracțiunilor asociate plăților online. Pentru aceasta se impune o instruire adecvată a personalului ce lucrează în gestionarea plăților online, indiferent de sectorul de activitate.

Deși plățile online se întâlnesc în toate tipurile de activități de comerț online, jocurile de noroc online prezintă cele mai multe riscuri asociate plăților online. Motivele ar putea fi încadrate în două categorii:

a. Operatorii de jocuri de noroc, în goana după profit, coboară standardele de securitate pentru a avea cât mai multe încasări. De exemplu, majoritatea organizatorilor de jocuri de noroc online nu utilizează protocolul 3D Secure pentru plățile cu cardul, astfel încât este mult mai ușor de efectuat depuneri în contul de joc, fără o parolă suplimentară derivată din 3D Secure, dar asta înseamnă și un risc mai mare de folosire a cardurilor fără consimțământul

[4] Blogul GPec (17 ian 2017) opus citatum

titularului acestora. Un alt exemplu ar fi permiterea de depuneri în contul de joc de pe carduri aparținând altor persoane decât titularul contului de joc.

b. Prin natura activității sale, jocurile de noroc atrag infractorii într-o proporție mai mare decât alte tipuri de activități. Printre explicațiile posibile sunt cele de natură psihologică și cele de natură practică.

    b1) În cadrul motivațiilor psihologice se pot enumera acelea prin care contravenienții își justifică activitatea ilegală prin aceea că jocurile de noroc sunt ele însele injuste (sunt făcute să păcălească clienții) și deci e normal ca și clienții să încerce tot felul de matrapazlâcuri pentru a contrabalansa activitatea organizatorilor.

    b2) Alți infractori abordează latura practică a jocurilor de noroc, și anume că atunci când folosesc un card fără consimțământul titularului, este mai ușor să încerce să scoată banii de pe acel card prin intermediul unui operator de jocuri de noroc decât prin intermediul unei comerciant de produse electronice, de exemplu, pentru că în acel caz infractorul primește produsul electronic pe care trebuie apoi să-l comercializeze pe piața neagră pentru a intra în final în posesia banilor. În cazul jocurilor de noroc online, banii nu se mai transformă în alte produse, ci pot fi retrași din contul de joc într-un alt cont controlat de infractor.

În concluzie, pentru prevenirea și combaterea infracțiunilor legate de plățile online pentru jocuri de noroc este necesară angajarea de personal calificat, cu o instruire corespunzătoare și continuă, pentru a fi mereu la curent cu noutățile din domeniu și cu riscurile asociate acestora. De aceea a fost concepută tema de cercetare curentă, și anume „Dezvoltarea resurselor umane în vederea optimizării securității plăților online”.

i) Actualitatea și oportunitatea cercetării

Tema de cercetare este de mare actualitate deoarece comerțul electronic înregistrează creșteri considerabile în fiecare an (30% creștere în 2016 comparativ cu 2015 și 20% creștere în 2015 comparativ cu 2014 conform studiului GPeC citat anterior) și face parte din ce în ce mai mult din viața noastră. Deja trăim într-o lume digitală, interconectată, în care informația se propagă rapid în toată rețeaua. Mai mult, de curând a apărut conceptul „Internetul pentru toate lucrurile”

sau ”Internetul pentru obiecte” (în limba engleză ”Internet of Things[5]”), adică din această lume digitală (interconectată) vor face parte și lucruri, nu numai oameni. De exemplu, deja se vorbește despre frigidere inteligente care vor putea plasa comenzi online pentru produsele consumate, pentru a reîntregi stocul. Toată această tehnologie vine însă la pachet atât cu avantaje, cât și cu riscuri emergente. Infractorii cibernetici vor găsi noi posibilități de a păcăli frigiderul din exemplul nostru și de a deturna fondurile care fac obiectul plăților online către destinații ilicite și controlate de infractori. Până să ajungem la acel nivel, totuși chiar și în zilele noastre tehnologia a avansat atât de mult că există posibilitatea de a filma un card, chiar și în timp ce este în mâinile posesorului său, cu un dispozitiv mic, înglobat chiar în ochelari, și practic în acel fel se pot fura datele cardului fără a se fura cardul în sine (plasticul), ci doar informația (datele scrise pe card). Cum posesorul cardului nu este conștient că i s-a furat cardul, nu va face eforturi urgente pentru a-l bloca. Astfel, infractorul poate folosi datele cardului la alte cumpărături online. Mult mai târziu, după ce bunurile sau serviciile cumpărate cu cardul respectiv au fost livrate, în momentul în care posesorul cardului constată tranzacții suspecte pe extrasul de cont, poate face reclamație la bancă („refuz la plată”), pe motiv de fraudă (tranzacții neautorizate). Dacă banca acceptă cererea de refuz la plată, atunci comerciantul, care a livrat deja bunurile sau serviciile, este nevoit să returneze banii încasați, ceea ce îi provoacă pierderi. Am detaliat aceste aspecte în studiul de caz din capitolul VI.

În acest context, oportunitatea cercetării apare ca necesitate a implementării unor măsuri adecvate de securitate în ceea ce privește plățile online, și cu cât mai repede, cu atât mai bine. Este așadar necesară instruirea personalului care operează activități de plăți online pentru instalarea, monitorizarea și îmbunătățirea sistemelor de securitate a plăților online.

ii) Scopul și obiectivele cercetării

În această lucrare doctorandul consideră cercetarea ca fiind un proces sistematic în care se colectează date (informații) ce sunt analizate urmând a se formula concluzii (rezultatele cercetării) pentru îmbunătățirea înțelegerii noastre asupra diverselor situații cu care ne confruntăm.

Cercetarea se realizează cu ajutorul unor metode științifice care presupun identificarea problemei, formularea unor ipoteze (posibile rezolvări ale problemei) și testarea acestora prin colectarea și analiza datelor, conform unor proceduri de raționament deductiv.

[5] Harvard Business Review , Internet of Things: Science Fiction or Business fact?, disponibil online la https://hbr.org/resources/pdfs/comm/verizon/18980_HBR_Verizon_IoT_Nov_14.pdf și accesat la 22.08.2017, orele 12:43

Așadar, cercetarea începe cu definirea clară a unui probleme, iar scopul cercetării este intenția de a găsi o rezolvare a acesteia.

În lucrarea de față problema identificată este cea care rezultă din raportările statistice menționate anterior și anume faptul că, deși comerțul electronic crește considerabil de la an la an, totuși plățile online cu cardul reprezintă un procent foarte mic (6%) raportat la comenzile online, pentru că majoritatea utilizatorilor preferă mijloace de plată mai sigure, cum ar fi plata ramburs sau la livrare, ca în 90% din cazuri. Problema este că într-o lume din ce în ce mai digitală cum este cea din zilele noastre, comenzile online nu pot fi numai pentru livrări de produse fizice pentru care se poate plăti ramburs, ci și pentru servicii (bilete de avion, rezervări la hotel, acces la platforme de joc sau educative etc.), care nu se livrează fizic și unde, de regulă, trebuie plătit înainte.

Astfel, scopul cercetării curente este acela de a optimiza securitatea plăților online (de a reduce incidentele de fraudă) prin instruirea adecvată a personalului comercianților care au de-a face cu plăți online.

Prin natura sa, scopul oricărei cercetări are o cuprindere destul de largă. Pentru a înainta către el avem nevoie de pași mai mici și mai concreți, sau, cu alte cuvinte, trebuie să definim obiectivele cercetării.

În general, obiectivele cercetării pot fi văzute drept enunțuri referitoare la rezultatele așteptate ale cercetării, în diverse etape de lucru sau din abordări diferite. Obiectivele sunt mult mai clar definite decât scopul, au caracteristici referitoare la unități măsurabile și sunt oportune, adecvate atingerii scopului.

Obiectivele cercetării de față sunt următoarele:

1) Înțelegerea factorilor psihologici care determină comportamentul infracțional pentru a construi mijloacele potrivite de combatere a acestuia;
2) Aprofundarea influenței mediului organizațional în schimbarea comportamentului individual și alunecarea către infracționalitate;
3) Identificarea principalilor factori de risc de fraudă și dezvoltarea programului de management al riscului de fraudă;
4) Înțelegerea caracteristicilor infracțiunilor de spălare de bani și de finanțare a terorismului;
5) Determinarea rolului resurselor umane în prevenirea și combaterea fraudei;
6) Identificarea unui domeniu care, prin natura activității sale, este mai expus riscului de fraudă cu cardul;

7) Înțelegerea modului de organizare a departamentului de risc și fraudă a unei societăți organizatoare de jocuri de noroc online;
8) Identificarea riscurilor de fraudă specifice jocurilor de noroc online;
9) Elaborarea de proceduri de lucru ca parte a instruirii personalului din domeniul jocurilor de noroc online;
10) Implementarea de măsuri concrete (cum ar fi introducerea protocolului 3D Secure) pentru a limita pierderile rezultate din frauda cu cardul bancar.

iii) Ipotezele de lucru

Odată stabilite obiectivele unei cercetări., acestea sugerează și niște posibile răspunsuri la problema care stă la baza cercetării. Aceste posibile răspunsuri se numesc ipoteze de lucru, iar cercetarea științifică se derulează în continuare prin testarea ipotezelor de lucru în urma colectării și analizei datelor, urmând a se formula concluziile (rezultatele cercetării) care pot confirma sau infirma ipotezele de lucru.

Ipotezele de lucru ale lucrării de față sunt:

1) Comportamentul infracțional apare în urma unui complex de factori psihologici și sociologici și este dificil de creat modele pentru a prevedea comportamentul infracțional, deoarece sunt foarte multe variabile care se modifică de la caz la caz;
2) Reducerea incidentelor de fraudă se poate face prin analizarea factorilor de risc de fraudă și prin implementarea de măsuri adecvate pentru diminuarea acelor riscuri;
3) Gradul de eficiență al analizei de risc, precum și de implementare de măsuri adecvate depinde de calitatea resurselor umane implicate. Prin urmare, se impun politici susținute de instruire a personalului ce lucrează în domeniul plățile online.
4) Implementarea unor măsuri concrete, cum ar fi introducerea protocolului 3D Secure, se poate face prin raportarea la media tranzacțiilor care au generat pierderi dintr-o perioadă de timp reprezentativă.

iv) Contribuții personale

Tema aleasă de doctorand este una nu numai de mare actualitate, dar și originală, ținând cont că sunt foarte puține alte lucrări în domeniu. Aceasta ar fi prima contribuție personală.

Deoarece frauda apare ca un fenomen multidisciplinar, cercetările de management al riscului de fraudă ar trebui extinse și corelate atât cu cercetări psihologice privind comportamentul deviant individual, cât și cu studii sociologice și organizaționale pentru a înțelege impactul organizației/ mediului asupra modelării comportamentului individual și vulnerabilitățile ce pot conduce la infracționalitate. Mai mult, odată comisă, frauda devine un caz penal și este abordată de domeniul juridic. Cercetarea de față corelează toate aceste aspecte multidisciplinare pentru a găsi soluția optimă, iar aceasta se prefigurează prin implementarea de măsuri de prevenire a fraudei în funcție de factori de risc de fraudă identificați. Studiul multidisciplinar, precum și abordarea soluției de prevenire în funcție de risc constituie și ele contribuții personale ale doctorandului.

Mai departe, doctorandul a identificat un domeniu de activitate cu risc crescut de fraudă la plățile online cu cardul, și anume jocurile de noroc online. Pentru acest domeniu distinct, pe baza experienței practice, dar și în urma certificărilor profesionale pe care le-a obținut, (CFE – Certified Fraud Examiner, AML Trainer, a se vedea Anexele), doctorandul a propus proceduri specifice de lucru ca parte a procesului de instruire a personalului. Aceste proceduri sunt detaliate în capitolele IV și V, iar responsabilitățile ce decurg din aplicarea lor au fost adăugate de doctorand în fișele de post reale, folosite în piață de un operator de jocuri de noroc și incluse în Anexe. Tot în Anexe doctorandul prezintă un material de instruire a personalului pentru prevenirea și combaterea spălării de bani, material la care este co-autor.

Mai mult, în capitolul VI, doctorandul efectuează un studiu caz pe date reale din piață pentru a stabili concret cum se poate implementa o măsură de securitate distinctă, și anume protocolul de plăți 3D Secure. În urma studiului de caz, și mai precis în urma analizei statistice descriptive a bazei de date a reieșit că tendința centrală (în cazul respectiv media, văzută sub forma unei curbe de regresie) nu este reprezentativă și, implicit, repartiția probabilistică normală a seriei de date nu descrie corect comportamentul întregii populații statistice. În acest context, doctorandul demonstrează că nu orice acțiune trebuie analizată doar prin prisma mediei, ci trebuie căutate alte repere concludente fiecărei situații în parte. Pentru studiul de caz din capitolul VI, doctorandul propune, tot ca o contribuție personală, folosirea mediei ponderate pentru a se vedea impactul fiecărui tip de tranzacție în totalul tranzacțiilor, izolând astfel tranzacțiile cu impact reprezentativ și introducând protocolul 3D Secure numai pentru acele tranzacții riscante.

Nu în ultimul rând, o altă contribuție personală este aceea că, în cadrul expunerii teoriei, doctorandul vine cu exemple ilustrative, derivate din cercetarea personală, cum ar fi, în cadrul

secțiunii 1.1.4 de dezvoltare a resurselor umane, mențiunile procedurilor specifice ale firmei de curierat UPS în care șoferii au rutele stabilite în așa fel încât efectuează doar viraje la dreapta, pentru a evita problemele derivate din cedarea trecerii (și a pierderii timpului) la virajele la stânga, sau procedurile specifice lanțului de cafenele Starbucks care lasă să curgă apa la chiuvete tot timpul pentru a diminua, susțin ei, riscul de contaminare a apei cu bacterii.

v) Metodologia cercetării

Cercetarea de față a folosit mai multe metode de lucru. Mai întâi, metoda inductivă[6] este implicită pentru că observațiile efectuate la nivelul domeniului de jocuri de noroc se pot extinde (prin cercetări ulterioare) către alte domenii unde se procesează plăți online. Domeniul jocurilor de noroc online este unul unde incidența fraudei cu cardul este destul de ridicată și se aceea se pretează studiului pentru prevenire și combaterea fraudei în plățile online în general, nu numai în domeniul jocurilor de noroc.

Mai departe, metoda analizei și sintezei s-a făcut prin descompunerea și studierea tuturor conceptelor mari care generează factori de risc de fraudă (și spălare de bani), prin identificarea respectivilor factori de risc, urmând ca, în final, să se facă recompunerea întregului edificiu teoretic prin prisma modului de răspuns la factorii de risc identificați.

Conceptele supuse analizei prin descompunere sunt „managementul resurselor umane", „riscul și managementul riscului", precum și „organizațiile și mediul lor", inclusiv „cultura organizațională". Dintre acestea, „managementul resurselor umane" are o greutate mai mare pentru că lucrează și acționează direct asupra angajaților, începând cu faza de selecție (cu accent pe istoricul persoanei, în engl. „background check"), apoi cu faza de formare și perfecționare profesională.

În studiul de caz din capitolul VI, metoda de bază a fost analiza-diagnoză. Nicio recomandare sau soluție nu poate veni fără o analiză temeinică a situației de fapt (a problemei). În urma analizei vor rezulta niște concluzii (un diagnostic) și pe baza acestor concluzii se vor face recomandări pentru a se ajunge la scopul urmărit, respectiv reducerea pierderilor din refuzurile la plățile cu cardul, dar fără a auto-gâtuire a veniturilor ce va genera practic alte pierderi din

[6] Research Methods – Knowledge base, disponibile online la https://www.socialresearchmethods.net/kb/dedind.php și accesate la 22.08.2017, orele 18:17.

neîncasarea veniturilor (posibil chiar mai mari decât înainte). Recomandările vor specifica de la ce nivel al sumei depuse în sus se poate introduce protocolul 3D Secure.

În cadrul studiului de caz, analiza-diagnoză ocupă cel mai mult spațiu, deoarece concluziile și recomandările pot fi făcute în doar câteva rânduri. Analiza propriu zisă este mult mai laborioasă și va implica sub-metode cum sunt analiza statistică descriptivă a bazei de date pentru a determina dacă tendința centrală (media, sub formă de curbă de regresie) este reprezentativă pentru seria de date statistice și dacă implicit repartiția probabilistică normală descrie corect comportamentul întregii populații de date statistice.

vi) Structura cercetării

Cercetarea este structurată în șase capitole. În capitolul I sunt prezentate aspecte teoretice referitoare la resurse umane și la mediul ambiant al organizației. Prima secțiune a capitolului prezintă fundamente teoretice ale Managementului Resurselor Umane în prevenirea și combaterea fraudei. Sunt definite principalele concepte, sunt trasate obiectivele și sunt punctate cele patru funcții ale managementul resurselor umane: asigurarea, menținerea, dezvoltarea și motivarea resurselor umane. Fiecărei funcții i se alocă o sub-secțiune. În partea a doua a capitolului întâi se prezintă aspecte teoretice ale organizației și mediul său, inclusiv cultura organizațională. Capitolul I se încheie cu vulnerabilități ale organizației privind activitatea infracțională, care face trecerea către capitolul II.

În capitolul II, secțiunea întâi, se analizează comportamentul organizațional începând cu principalele elemente care îl formează, respectiv individul, grupul, organizația, plus relațiile dintre ele, inclusiv relația cu mediul extern. Mai departe, sunt analizate modelele comportamentului organizațional și găsită o corelație dintre acestea și ierarhia nevoilor individuale a lui Maslow. Secțiunea a doua a începe cu prezentarea celor mai importante teorii comportamentale, respectiv teoria ranforsării și pedepsei a lui Skinner. Sunt detaliate resorturile psihologice care pot sta la baza declanșării unui comportament deviant, ca feedback din partea stimulilor externi. Mai departe, este căutat răspunsul la întrebarea „De ce unii oameni respectă legile, iar alții nu?”, mergând pe linia studiului lui Tyler, care a constatat că oamenii respectă legile în special dacă legiuitorul are legitimitate, respectiv dacă acționează într-un cadru considerat just, echitabil sau „fair”. Sunt apoi reliefate cele 6 criterii ale sociologului american Leventhal pe baza cărora oamenii judecă dacă ceva este just sau nu, și anume: reprezentativitatea, consecvența, lipsa ideilor

preconcepute și/sau a conflictului de interese, acuratețea, corectitudinea și nivelul de etică. În secțiunea a treia din capitolul II sunt analizate principalele teorii infracționale, respectiv cele care încearcă să explice comportamentul infracțional. Acestea sunt destul de numeroase, pentru că niciuna nu poate oferi o explicație universal valabilă. Categorisirea este făcută în teorii clasice, respectiv cele care avansează conceptul de utilitarism și în cazul infractorilor, care urmăresc maximizarea plăcerii și minimizarea suferinței, în teorii sociale, care analizează efectele acumulării de tensiuni sociale în diverse circumstanțe de relaționare și apartenență dintre individ (plus crezurile sale) și mediu, și în teorii ale omului modern, care investighează consecințele înstrăinării indivizilor de viața reală și participarea la cea virtuală prin intermediul rețelelor de socializare și a internetului. În secțiunea a patra este analizată așa numita infracțiune a gulerelor albe, adică cea legată de locul de muncă. Se distinge ideea că organizațiile pot pune presiune pe indivizi pentru a le schimba comportamentul, ceea ce ar conduce chiar la comiterea de infracțiuni.

Capitolul III începe cu prezentarea noțiunilor teoretice referitoare la risc, reacția la risc și managementul riscului, și continuă cu prezentarea de cercetări curente ale stadiului implementării măsurilor de management al riscului. În secțiunea a treia a capitolului III sunt prezentate obiectivele programului de management al riscului de fraudă, conform standardelor internaționale (ISO), iar în ultima secțiune a capitolului III este descrisă dezvoltarea programului de management al riscului de fraudă.

În prima secțiune a capitolului IV sunt prezentate, separat, conceptele de spălare de bani și de finanțare a terorismului. Se formulat ideea că spălarea de bani este foarte utilă în descoperirea altor fraude, ascunse, care au produs „banii negri" ce trebuie spălați. De asemenea, este evidențiată principala diferențiere între spălare de bani și finanțarea terorismului, și anume aceea că, dacă în cazul spălării de bani avem întotdeauna de-a face cu surse ilicite de venituri, în cazul finanțării terorismului se întâlnesc, de regulă, surse perfect licite. De aceea, pentru descoperirea finanțării terorismului trebuie avute în vedere alte metode de lucru. În ultima parte a secțiunii întâi a capitolului IV este reliefat atât rolul (cum face), cât și locul (ce face) managementului resurselor umane în prevenirea și combaterea fraudei. Cum frauda poate fi atât internă (săvârșită de proprii angajați), cât și externă (comisă de clienți, furnizori, terți), departamentul de resurse umane se preocupă de monitorizarea angajaților pentru a preveni frauda internă și de implementarea de proceduri de lucru specifice pentru prevenirea și combaterea fraudei externe. În introducerea de la secțiunea a doua a capitolului IV, doctorandul identifică domeniul jocurilor de noroc online ca

fiind unul cu risc ridicat de fraudă la plățile online cu cardul. În continuare, în secțiunea a doua se prezintă situația jocurilor de noroc online din România și a societăților comerciale autorizate să furnizeze astfel de servicii. Mai departe este descris departamentul de risc și plăți online al unei societăți comerciale din sectorul jocurilor de noroc online. Sunt prezentate posturile de lucru (inclusiv fișa postului, în Anexe), procedurile de lucru precum și materiale de instruire a personalului, atât pentru prevenirea și combaterea fraudei, cât și a spălării de bani. În secțiunea a treia a capitolului IV sunt elaborate, separat, proceduri specifice pentru diminuarea riscului de fraudă și proceduri specifice pentru diminuarea riscului de spălare de bani. De asemenea, sunt întocmite procedurile de lucru pentru fiecare post din cadrul departamentului de plăți online, respectiv procedurile de lucru ale agentului de validare documente, procedurile de lucru ale agentului de plăți online și procedurile de lucru ale agentului de risc și anti-fraudă.

În capitolul V sunt trecute în revistă toate tipurile de risc asociate plăților la jocurile de noroc online, împărțite pe categorii (riscul financiar, riscul la depunere, riscul operațional, riscul pierderii procesatorului de plăți, riscul reputației, riscul de neconformitate cu legea și riscul pierderii lichidității). Pentru depunerile cu cardul sunt detaliate și alte riscuri specifice, cum ar fi cele asociate cardurilor, cele asociate jucătorilor și cele asociate dispozitivelor de comunicare. În a doua jumătate a capitolului V sunt evidențiate măsurile de răspuns la riscurile identificate în prima jumătate a capitolului.

În capitolul VI se prezintă un studiu de caz cu date reale în care se caută reducerea pagubelor apărute în urma folosirii frauduloase a cardurilor (refuzuri la plată sau „chargebacks”). Datele recepționate de la o firmă reală din România sunt analizate din punct de vedere statistic (medie, mediană, mod, dispersie, abatere medie pătratică, coeficient de variație, repartiție probabilistică normală, coeficienți de variație (Pearson) etc.) pentru a se determina dacă tendința centrală (media) este reprezentativă pentru toată seria de date, dacă aceasta reprezintă a curbă de regresie acceptabilă pentru întreaga serie. Cum tendința centrală (media) nu este reprezentativă pentru seria de date în cauză, se trece mai departe la analiza impactului (media aritmetică ponderată) pe diferite praguri și se găsește un interval optim pentru introducerea protocolului 3D Secure în așa fel încât auto-gâtuirea să nu producă pagube mai mari prin neîncasarea veniturilor decât erau cele din fraudă, înainte de introducerea 3D Secure. Concluziile au fost prezentate firmei ordonatoare a studiului cu grad de recomandări pentru implementare în practică.

vii) Limite și cercetări ulterioare

Definirea unor obiective concrete, măsurabile înseamnă și delimitarea lor, adică introducerea unor limite pentru orice cercetare. În cazul de față, principala limită este aceea că implementarea concretă de măsuri anti-fraudă bazate pe factori de risc specifici s-a realizat numai pentru comercianți din domeniul jocurilor de noroc. Totuși, comerțul electronic acoperă majoritatea domeniilor de activitate, fiecare cu riscurile sale specifice.

De exemplu, un alt sector expus fraudei cu cardurile bancare este cel de retail online. Principalii furnizori de astfel de servicii la nivel mondial sunt Amazon.com și alibaba.com. În Romania un astfel de furnizor este eMag.ro. Pentru aceste tipuri de servicii există riscul ca un client să comande și să plătească folosind un card furat, iar furnizorul să se confrunte cu reclamația adevăratului posesor al cardului după ce a livrat deja bunurile comandate. Conform reglementărilor din domeniul plăților online, comerciantul (furnizorul) este obligat să returneze banii înapoi pe cardul furat, însă cum bunurile au fost deja trimise, practic comerciantul realizează o pierdere (pagubă). De cele mai multe ori pierderea este irecuperabilă sau are costuri de investigare și recuperare ce depășesc valoarea produselor livrate. Pentru acest domeniu de activitate se impun alte analize de risc ce pot face obiectul unor cercetări ulterioare.

Un alt exemplu de sector de activitate expus fraudei la plata online este cel de comerț second-hand online. Unul dintre principalii furnizori la nivel mondial este ebay.com, iar în România cei mai reprezentativi competitori sunt olx.ro, okazii.ro, publi.24.ro, lajumate.ro. Practic, orice site de anunțuri poate fi transformat în platformă de comerț online second-hand. Din cercetările preliminare ale doctorandului, aceste platforme nu se preocupă prea mult de asigurarea securității tranzacțiilor, astfel că, dacă un cumpărător comandă un produs de pe platformă și îl plătește în avans, platforma nu face eforturi de a asigura livrarea acelui produs către cumpărător în condițiile anunțului. Sunt multe cazuri menționate în media sau pe rețelele de socializare în care cumpărătorii de pe astfel de site-uri s-au plâns că au plătit, dar nu au primit produsul, deci au fost fraudați. Doctorandul vede aici o oportunitate reală de a implementa măsuri de securitate pentru plățile online în avans, cum ar fi, de exemplu, introducerea unui sistem de gaj asigurat de platforma online astfel încât banii nu sunt trimiși direct la vânzător, ci sunt reținuți temporar, într-un cont de gaj, de către platforma online, urmând a fi virați vânzătorului după ce cumpărătorul confirmă recepția corespunzătoare a produsului comandat. Invers, pentru a proteja vânzătorul că trimite produsul, dar nu încasează banii, platforma online va solicita ca mai întâi cumpărătorul să vireze

banii către platforma online și apoi vânzătorul livrează produsul. În acest moment, pe piață nu există un sistem de securitate clar definit și implementat (platformele care oferă astfel de servicii au chiar un „disclaimer” prin care își declină responsabilitatea actului de comerț între cumpărător și vânzător) și, prin urmare, doctorandul vede reale oportunități de cercetare și implementare de măsuri se securitate a plăților online pentru aceste platforme de comerț online second-hand.

INFORMAŢII PERSONALE

Marius Burcă

Aleea Stănilă nr. 5, Bl. H7, Sc. C, Ap. 57, Sector 3, București

0721856205

mariusburca@yahoo.com

Sexul Masculin | Data naşterii 09/11/1972 | Naţionalitatea română

STUDIILE PENTRU CARE SE CANDIDEAZĂ

Doctorat în Management

EXPERIENŢA PROFESIONALĂ

din iulie 2015 - până în prezent

Manager marketing/ Auditor de risc și plăți online

SC Bet Zone SRL

- Crearea și implementarea strategiei de marketing a societății comerciale
- Crearea și dezvoltarea Departamentului de Risc și plăți online
- Angajarea și instruirea personalului

Tipul sau sectorul de activitate jocuri de noroc online

din noiembrie 2011 - până în iulie 2013

Manager de Proiect

Sumup Limited (www.sumup.com)

- Asigurarea conformității cu legislațiile din Irlanda, Marea Britanie și Germania pentru firmele procesatoare de plăți online cu cardul
- Crearea și implementarea politicilor de prevenire fraudelor și a spălării de bani
- Supravegherea tranzacțiilor companiei

Tipul sau sectorul de activitate IT, plăți cu cardul

din martie 2007 - până în februarie 2012

Consultant marketing

Earthquake Media

- Asigurarea conformității cu legislația din România pentru jocurile de noroc online
- Implementarea politicilor de marketing ale clientului în România
- Supravegherea activității clienților pentru depistarea fraudelor și prevenierea spălării de bani

Tipul sau sectorul de activitate IT, jocuri de noroc online

din aprilie 2002 - până în iulie 2013

Administrator

Gamebookers Divertisment SRL

- Asigurarea conformității cu legislația din România în ceea ce privește activitatea cu Licență de la Ministerul Finanțelor în domeniul caselor de pariuri sportive
- Crearea și implementarea politicilor de marketing ale companiei
- Implementarea politicilor de prevenire fraudelor și a spălării de bani
- Supravegherea politicii de personal
- Supravhegherea activității financiar-contabile
- Consultarea juriștilor externi pe probleme legale

Tipul sau sectorul de activitate jocuri de noroc

EDUCAŢIE ŞI FORMARE

din 1999 – până în 2001

Master in Ingternational Business

Norwegian School of Economics and Business Administration, Bergen, Norvegia

- Masterul este echivatentul unui MBA cu focus pe relații economice internaționale

din 1991 – până în 1996

Studii de licență

ASE București, Facultatea de Relații Economice Internaționale

- Studii de 5 ani

COMPETENTE PERSONALE

Limba(i) maternă(e): română

Alte limbi străine cunoscute

	INTELEGERE		VORBIRE		SCRIERE
	Ascultare	Citire	Participare la conversaţie	Discurs oral	
Engleză	C2	C2	C2	C2	C2
	Cambridge CPE, Grade B				
Franceză	A1	A2	A1	A1	

Niveluri: A1/2: Utilizator elementar - B1/2: Utilizator independent - C1/2: Utilizator experimentat
Cadrul european comun de referinţă pentru limbi străine

Competenţe de comunicare
- bune competenţe de comunicare dobândite prin experienţa internațională de relații cu parteneri. clienți, investitori, autorități de reglementare

Competenţe organizaţionale/manageriale
- leadership (am condus un lanț de agenții de pariuri sportive cu peste 10 angajați)
- am deschis filiala de la Amsteram a companiei Sumup Limited
- am fondat două societați comerciale în România

Competenţe dobândite la locul de muncă
- o bună cunoaştere a politicilor de conformitate în domeniul plăților online și al jocurilor de noroc
- o bună înțelegere a teoriei probabilităților

Competenţe informatice
- o bună cunoaştere a instrumentelor Microsoft Office™ și a programului Adobe Fireworks
- cunoștințe de HTML, CSS
- cunoștințe de SQL

Permis de conducere: Categorie
- B

INFORMATII SUPLIMENTARE

Afilieri
- Membru afiliat (nr. 674613) al Association of Certified Fraud Examiners, Houston, Texas

Referinţe
- Marine Jouaillec, former Legal adviser, SumUp Limited, mobile +33661489501, email marinejouaillec@gmail.com
- Michael Maerz, former Director of Sportsbetting, Party Gaming, mobile +35058009382, email maerzmichael@yahoo.com
- Piotr Blazewicz, former Regional Manager, Party Gaming, mobile +34654499653, email piotr.blazewicz@gmail.com

DATA: 06.12.2017 **SEMNĂTURA:**

Lista articolelor publicate și a participărilor la conferințe

Nr. crt	Numele și prenumele doctorandului	Denumire articol	Autori	Conferința internațională	Luna desfășurării conferinței	Website
1.	BURCĂ Marius	New trends in combatting fraud and money laundering: Social Status Laundering	BURCĂ Marius	Management and Innovation for Competitive Advantage, 5-6 November 2015, Bucharest, Romania	5-6 Noiembrie	http://conference.management.ase.ro/
		Presiuni ale culturii organizaționale către fraudă - o abordare interdisciplinară dinspre management, psihologie, sociologie și criminologie	BURCĂ Marius	Conferința internă a proiectului POSDRU/187/1.5/S/155463 din data de 20-21 noiembrie 2015, de la ASE București	20-21 Noiembrie	http://interdisciplinar.ase.ro/Media/Default/documente/conferinta/Program_Conferinta%2020-21_noiembrie_2015_final.pdf
		Market pressure and combating fraud in the online gaming industry – is the reconciliation possible?	BURCĂ Marius	Global Interferences of Knowledge Society 7-8 October 2016, Târgoviște, România	7-8 Octombrie	
		The Real Danger Behind the Offshore Business: Identity Laundering	BURCĂ Marius	Journal of US-China Public Administration	March 2016, Volume 13, Number 3, serial Number 125	ISSN 1548-6591

SEMNĂTURA:

MINISTERUL EDUCAŢIEI NAȚIONALE
UNIVERSITATEA „VALAHIA” din TÂRGOVIŞTE - IOSUD
Str. Lt. Stancu Ion, Nr. 35 – 130105, Târgovişte, România
Tel/Fax: +40-245-206104
http://scoaladoctorala.valahia.ro/

DOCTORAL THESIS:

Human resource development to optimise the security of online payments

PhD Supervisor:
Prof.univ.dr. Mohammad JARADAT

PhD Student:
Marius BURCĂ

TÂRGOVIŞTE
2018

TABLE OF CONTENTS

KEYWORDS

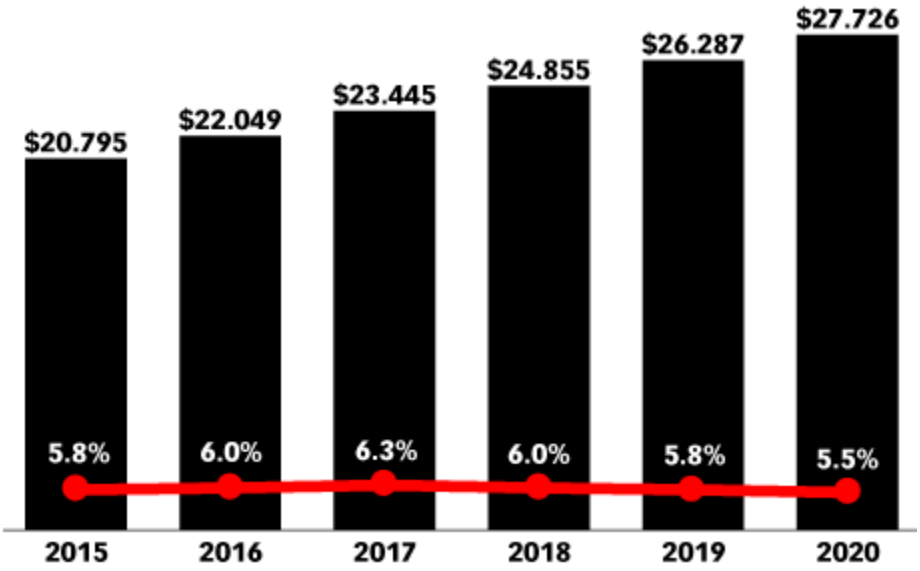
Online payments
Human resources development
Anti-fraud
Money laundering
Online payments risk management
Organizational behaviour
Gambling
Behaviour analysis
White collar crime

THESIS SUMMARY

With the globalization and the emergence of the Internet, e-commerce continues to grow and keep an increasingly important role in our lives. The worldwide volume of transactions in 2016 amounted to 22,049 thousand dollars, up 6% compared to the year 2015, according to a marketing survey[1].

The same study forecasts that the annual growth rate will be maintained by 2020:

Figure 1 – World e-commerce trends



(Source: eMarketer[2])

In Romania e-commerce is steadily increasing, as well. A GpeC[3] study shows that in the year 2016 the online shopping volume went up to 1.8 billion euros, which is an increase of 30% compared to 2015. The same study estimates that there are 11.2 million internet users in our country, ensuring a penetration rate of 58% of the total population.

---

[1] Emarketer (22 Aug 2016), „Worldwide Retail Ecommerce Sales Will Reach $1.915 Trillion This Year", available online at https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369 and visited on 21.08.2017, 17:32 hours

[2] Emarketer (22 Aug 2016) opus citatum

[3] Blog GPec (17 Jan 2017) available online at http://www.gpec.ro/blog/bilantul-pietei-de-e-commerce-2016-romanii-au-cumparat-online-de-peste-18-miliarde-de-euro-infografic and visited on 22.08.2017, 10:42 hours

Of the 11.2 million internet users, 6.7 million made online shopping at least once in 2016, and 2.34 million used a mobile device (phone, tablet).

However, of the total online shopping, only 6% were made with the bank card, although some 14.5 million cards are issued. As a matter of fact, 90% of online payments were made through cash on delivery, and the remaining 4% by other methods (online banking, micro-payments via SMS, etc.).

Table 1 – Methods of payment in ecommerce in Romania in 2016

Method of payment	**Percentage weight**
Cash on delivery	90,00%
Online payment – Credit Card	6,00%
Others (online banking, SMS, eWallet)	4,00%

(Sursa GPeC[4])

The data above shows the reluctance of bank card users to use them for online payments, and rightly so: online card payments pose risks.

In this context, in order to keep pace with the evolution of e-commerce, all entities involved in online payments (both merchants and online payment processors) must provide sufficient methods to prevent and combat offenses related to online payments. This requires proper training of staff working in online payments, regardless of the industry.

Although online payments are found in all types of online business, online gambling presents the most risks associated with online payments. The reasons could be divided into two categories:

a. Gambling operators, in the pursuit of profit, lower security standards to get as much revenue as possible. For example, most online gambling organizers do not use the 3D Secure protocol, so it's much easier to make deposits into gaming accounts without an extra

[4] Blogul GPec (17 ian 2017) opus citatum

password derived from 3D Secure, but that also means a higher risk of using credit cards without the consent of their owner. Another example would be to allow deposits from cards belonging to other persons than the gaming account holder.

b. By nature, gambling attracts offenders to a greater extent than other types of activity. Possible explanations are both psychological and practical.

b1) Psychological motivations include those where offenders justify their illegal activity by the fact that gambling is unfair by itself (gambling is only made to trick the players) and it is normal for players to try all sorts of shady actions to counterbalance the activity of the organizers.

b2) Other criminals address the practical side of gambling, that when using a card without the consent of the holder, it is easier to try to take the money off that card through a gambling operator than through an online shop, for example, because in that case the offender receives the product and then has to sell it on the black market to finally get the money. In the case of online gambling, the money does not turn into other products, and it can be withdrawn from the gaming account into a bank account controlled by the offender.

To conclude, for the prevention and combating of online gambling crimes, it is necessary to employ qualified staff with appropriate and continuous training to keep up-to-date with the online payments and with their associated risks. That is why the current research theme, namely "Developing Human Resources to Optimizing Online Payment Security", has been realized.

i) Opportunity of the research

The research topic is very hot because e-commerce is growing considerably each year (30% increase in 2016 compared to 2015 and 20% increase in 2015 compared to 2014 according to the GPeC study quoted above) and is increasingly part of our life. We are already living in an interconnected digital world where information is rapidly spreading across the network. Moreover, the concept of "Internet of Things[5]" has been developing lately, meaning that in this digital and

[5] Harvard Business Review, Internet of Things: Science Fiction or Business fact?, available online at https://hbr.org/resources/pdfs/comm/verizon/18980_HBR_Verizon_IoT_Nov_14.pdf and visited 22.08.2017, 12:43 hours

interconnected world there will be also things, not just people. For example, we are already talking about smart refrigerators that will be able to place online orders for consumed products to rebuild the stock. All this technology comes packaged with both advantages and emerging risks. Cyber criminals will find new possibilities to fool the refrigerator of our example and to divert funds from online payments to illicit destinations.

Until we reach that level though, even nowadays technology has so far advanced that there is the possibility of filming a card, even while it is in the hands of its owner, with a small device embedded in glasses, and basically in this way you can steal the card data without stealing the card itself (plastic), but just the information (the data written on the card). As the cardholder is not aware that his card has been stolen, he will not make urgent efforts to block him. Thus, the offender can use card data for other online shopping. A lot later, after the goods or services purchased with that card have been delivered, when the cardholder finds suspicious transactions on the bank statement, he can complain to the bank ("refusal to pay") for fraud (transactions unauthorized). If the bank accepts the request for refusal to pay, then the merchant, who has already delivered the goods or services, has to return the collected money, which causes it to lose. We have detailed these aspects in the case study in Chapter VI.

Hence, the opportunity for research appears as a necessity to implement adequate security measures for online payments, and as soon as possible, the better. It is therefore necessary to train staff which is involved in online payments and to install, monitor and improve online payment security systems.

ii) The purpose and objectives of the research

In this paper, the PhD student considers “research” as a systematic process in which the data (information) that is being analyzed is collected, and conclusions (research results) are drawn to improve our understanding of the various situations we face.

The research is carried out by using scientific methods that involve identifying the problem, formulating hypotheses (possible solutions to the problem) and testing them by collecting and analyzing the data according to deductive reasoning procedures.

So, research begins with a clear definition of a problem, and the purpose of research is to find a solution to it.

In the present paper, the problem identified is that resulting from the above-mentioned statistical reports, namely that although e-commerce is growing considerably from year to year, online card payments represent a very small percentage (6%) of the online orders, because most users prefer more secure means of payment, such as cash payment on delivery, as in 90% of cases. The problem is that within an increasingly digital world like today, online orders can not only be for supplies of physical products for which cash on delivery can be made, but also for services (flight tickets, hotel reservations, access to game or educational platforms etc.) which is not physically delivered and which, as a rule, must be paid in advance.

Thus, the purpose of current research is to optimize the security of online payments (to reduce fraud incidents) by properly training the staff which are dealing with online payments.

By its nature, the purpose of any research has a fairly wide scope. In order to move towards it, we need smaller and more concrete steps, or in other words, we need to define the objectives of the research.

In general, research objectives can be seen as statements about expected research outcomes at different work steps or from different approaches. Objectives are much more clearly defined than purpose, have characteristics related to measurable units and are timely, appropriate to achieving the goal.

The objectives of this research are:

1) Understanding the psychological factors which determine the criminal behavior in order to build the appropriate means to combat it;
2) Grasping the influence of the organizational environment on the change of individual behavior and the slip towards criminality;
3) Identifying the main fraud risk factors and the development of fraud risk management program;
4) Understanding the characteristics of money laundering and terrorist financing crimes;
5) Determining the role of human resources in preventing and combating fraud;
6) Identifying an area that, by its nature, is more exposed to the risk of card fraud;
7) Understanding the risk and fraud department structure of an online gambling company;
8) Identifying online gambling fraud;
9) Elaboration of working procedures as part of the staff training in the field of online gambling;

10) Implementing concrete measures (such as introducing the 3D Secure Protocol) to limit the loss resulting from bank card fraud.

iii) Working hypotheses

Once the objectives of a research have been established, they also suggest possible answers to the underlying question of research. These possible responses are called working hypotheses, and the scientific research is further developed by testing working hypotheses following data collection and analysis, and then by drawing conclusions (research results) that can validate (confirm) or invalidate (deny) the working hypotheses.

The working hypotheses of this paper are:

1) Criminal behavior arises from a complex of psychological and sociological factors and it is difficult to create models to predict criminal behavior as there are many variables that vary from case to case;
2) Reducing fraud incidents can be done by analyzing fraud risk factors and by implementing appropriate measures to mitigate those risks;
3) The degree of effectiveness of risk analysis, as well as the implementation of appropriate measures, depends on the quality of the human resources involved. Therefore, sustained policies are required to train staff working in the field of online payments.
4) Implementation of concrete measures, such as the introduction of the 3D Secure Protocol, can be done by reference to the average (mean) of transactions that generated losses over a representative period of time.

iv) Personal contributions

The topic chosen by the PhD student is not only hot but also an original one, considering that there are very few other papers in the field. That would be his first personal contribution.

Because fraud occurs as a multidisciplinary phenomenon, fraud risk research should be expanded and correlated with both psychological research of individual deviant behavior and sociological and organizational studies in order to understand the impact of the organization/ environment on how to shape individual behavior and vulnerabilities which can lead to crime. Moreover, once committed, fraud becomes a criminal case and is addressed by the legal field. This research correlates all these multidisciplinary aspects in order to find the optimal solution, and this

is prefigured by implementing fraud prevention measures based on identified fraud risk factors. The multidisciplinary study as well as the risk prevention approach are also personal contributions of the PhD student.

Furthermore, the PhD candidate identified a high-risk activity area for online card payments, namely online gambling. For this distinct field, based on the practical experience and the professional certifications he has obtained (CFE - Certified Fraud Examiner, AML Trainer, see Appendixes), the PhD student proposed specific working procedures as part of the personnel training. These procedures are detailed in Chapters IV and V whereas the responsibilities arising from their application have been added by the doctoral student to the actual job postings used in the market by a gambling operator and included in the Annexes. Also in the Appendices, the PhD candidate presents a training material for the personnel to prevent and combat money laundering, a material to which he is co-author.

Moreover, in Chapter VI, the PhD student conducts a case study on real market data to determine specifically how to implement a distinct security measure, namely the 3D Secure Payment Protocol. According to the case study, and more precisely following the descriptive statistical analysis of the database, it was revealed that the central trend (in this case the mean, seen as a regression curve) is not representative and, implicitly, the normal probability distribution of the series data does not correctly describe the behavior of the entire statistical population. In this context, the PhD student demonstrates that not all actions should be considered only in terms of the mean, and that other clues must be sought for each situation.

Therefore, for the case study in Chapter VI, the PhD candidate proposes the use of weighted average to see the impact of each transaction in the total transaction, as a personal contribution, thereby sealing transactions with a representative impact and introducing the 3D Secure Protocol only for those risky transactions.

Last but not least, another personal contribution is that, in the context of the theory, the PhD candidate comes up with illustrative examples derived from personal research, such as, in the section 1.1.4 (human resources development), the specific procedures of the courier operator UPS, in which drivers receive the routes so that they only make right turns in order to avoid problems (and time loss) of passing-through at the left-hand turns, or the Starbucks chain procedures to leave the water running from the sink at all times in order to diminish, they claim, the risk of water contamination with bacteria.

v) Research methodology

This research has used several working methods. First, the inductive method is implicit because gaming research can be extended (through further research) to other areas where online payments are processed. Online gambling is one industry where the incidence of card fraud is quite high, and it is therefore suitable for study of prevention and combating fraud in online payments in general, not only in gambling.

Further, the method of analysis and synthesis was carried out by dissolution and recompositing of all large concepts which generate fraud (and money laundering) by identifying the respective risk factors, and by taking the response actions to the identified risk factors.

The concepts analyzed by decomposition are "human resource management", "risk management" and "organizations and their environment", including "organizational culture". Of these, "human resource management" has more weight because it works and acts directly on employees, starting with the selection phase (with an emphasis on “Background check"), then going through the training and professional development phases.

In the case study of Chapter VI, the basic method was diagnosis analysis. No recommendation or solution can come without a thorough analysis of the factual situation. The analysis will result in some conclusions (a diagnosis), and on the basis of these conclusions, recommendations will be made to reach the intended goal, namely to reduce the loss from card payments chargebacks, and ideally without harming revenues as else it will actually generate other loss from non-collection of income (possibly even higher than before). The recommendations will specify at what level of deposit amount the 3D Secure Protocol can be introduced.

In the case study, the diagnosis-analysis takes the most space, because the conclusions and recommendations can be made in just a few lines. The actual analysis is more labor-intensive and will involve sub-methods such as the statistical descriptive database analysis to determine whether the central trend (the mean as a regression curve) is representative for the statistical data series and implicitly the normal probability distribution correctly describes the behavior of the entire population of statistical data.

vi) Research structure

The research is structured in six chapters. Chapter I presents theoretical aspects regarding human resources and the environment of the organization. The first section of the chapter presents

the theoretical foundation of Human Resource Management in preventing and combating fraud. The main concepts are defined, the objectives are outlined, and the four functions of human resources management are highlighted: ensuring, maintaining, developing and motivating human resources. Each function is assigned a sub-section. The second part of the first chapter presents the theoretical aspects of the organization and its environment, including organizational culture. Chapter I ends with vulnerabilities of the organization regarding criminal activity, which makes the transition to Chapter II.

In Chapter II, section one, organizational behavior is analyzed starting with the main elements that it forms, namely the individual, the group, the organization, plus the relations between them, including the relationship with the external environment. Further, we analyze the patterns of organizational behavior and find a correlation between them and Maslow's individual needs hierarchy. The second section begins with the presentation of Skinner's most important behavioral theories and Skinner's theory of reinforcement and punishment. Psychological spirals that can be the basis for triggering deviant behavior, as feedback from external stimuli, are detailed. The chapter continues with trying to find the answer to the question "Why do some people respect the law, and others do not?", by following the study of Tyler, who found that people respect laws especially if the legislator has legitimacy, or acts within a framework considered fair.

Next, we go through the six criteria of the American sociologist Leventhal, on the basis of which people judge whether something is fair or not, namely: representativeness, consistency, lack of preconceptions and/or conflicts of interest, accuracy, correctness and ethics.

The third section of Chapter II reviews the main criminal theories, namely those that try to explain the criminal behavior. These are quite numerous, because none can provide a universally valid explanation. The classification is made in:

- classical theories, namely those advancing the concept of utilitarianism and in the case of offenders, aiming to maximize pleasure and minimize suffering,

- social theories, which analyze the effects of accumulation of social tensions in different circumstances of relationship and belonging between the individual its) and the environment,

- modern human theories, investigating the consequences of alienating individuals from real life and participating in virtual life through social networks and the Internet.

The fourth section analyzes the so-called white-collar crime, i.e. the job-related offense. The idea is that organizations can put pressure on individuals to change their behavior, which would even lead to committing crimes.

Chapter III begins with the presentation of theoretical notions about risk, risk response and risk management, and continues with the presentation of current research on the state of implementation of risk management measures. The third section of Chapter III outlines the objectives of the fraud risk management program, in line with international standards (ISO), and the last section of Chapter III describes the development of the fraud risk management program.

In the first section of Chapter IV, the concepts of money laundering and terrorism financing are presented separately. The idea was that money laundering is very useful in discovering other hidden frauds that produced "black money" to be laundered. It also highlights the main distinction between money laundering and terrorist financing, namely that if money laundering is always a source of illicit income, terrorist financing is usually made from perfectly licit sources. That is why other working methods must be considered for identifying terrorist financing. In the last part of the first section of chapter IV, both the role (how) and the place (what) of human resources management in preventing and fighting fraud are highlighted. As the fraud can be both internal (committed by its own employees) and external (committed by customers, suppliers, third parties), the human resources department is concerned with employee monitoring to prevent internal fraud and with implementation of specific work procedures to prevent and combat external fraud.

In the introduction to the second section of Chapter IV, the PhD candidate identifies online gambling as being at a high risk of online card fraud. The second section presents the situation of online gambling in Romania and the companies authorized to provide such services. Then, the risk and online payments department of an online gambling company is described. Workplaces (including job description in annexes), working procedures and staff training materials are presented both for preventing and for combating fraud and money laundering. In the third section of Chapter IV separate procedures are developed to reduce the risk of fraud and specific procedures come into place to mitigate the risk of money laundering. Also, the work procedures for each job within the online payments department, such as the document validation agent working procedures, the online payment agent's working procedures, and the risk agent's and anti-fraud agent working procedures, are set up.

Chapter V lists all types of risk associated with online gambling payments, broken down into categories (financial risk, deposit risk, operational risk, loss of payment processor, reputational risk, risk of non-compliance with the law and risk of loss of liquidity). For card deposits, other specific risks, such as those associated with the cards themselves, then those associated with players, and finally those associated with communication devices, are detailed. The second half of Chapter V highlights the risk response measures identified in the first half of the chapter.

Chapter VI presents a case study with real data that seeks to reduce loss resulting from fraudulent use of cards ("chargebacks"). The data received from a real gambling operator in Romania is analyzed statistically (mean, median, mode, dispersion, standard deviation, coefficient of variation, normal probability distribution, variance coefficients (Pearson) etc.) to determine if the central trend (mean) is representative for the entire dataset, and if it represents the acceptable regression curve for the entire series. As the central trend (mean) turns out to not be representative for the data series in question, the study goes on to analyze the impact (weighted average) on different thresholds and finds an optimal threshold for introducing the 3D Secure protocol in such a way that it will not cause greater damage by not collecting revenues than the fraud loss amount before the introduction of 3D Secure. The conclusions were presented to the ordering company of the study together with recommendations for implementation in practice.

vii) Limits and further research

The definition of concrete, measurable objectives also means their delimitation, i.e. the introduction of limits for any research. In the present case, the main limit is that the concrete implementation of anti-fraud measures based on specific risk factors was made only for online gambling. However, e-commerce covers most areas of activity, each with its specific risks.

For example, another sector exposed to bank card fraud is online retail. The main providers of such global services are Amazon.com and alibaba.com. In Romania, such a provider is eMag.ro. For these types of services, there is a risk that a customer may order and pay using a stolen card and the provider will face the chargeback of the real cardholder after having already delivered the ordered goods. Under the online payments regulations, the merchant (the supplier) is required to return the money back to the stolen card, but as the goods have already been sent, the merchant actually makes a loss (damage). In most cases, the loss is irrecoverable or has investigative and

recovery costs that exceed the value of the products delivered. For this area of activity, other risk analyzes are required which may be subject to further research.

Another example of the industry exposed to online payment fraud is the second-hand online trade. One of the world's leading suppliers is ebay.com, and in Romania the most prominent competitors are olx.ro, okazii.ro, publi.24.ro, lajumate.ro. Basically, any ad site can be turned into a second-hand online trading platform. From the preliminary research of the PhD student, these platforms are not very concerned about ensuring transaction security, so if a buyer orders a product on the platform and pays it in advance, the platform does not make efforts to ensure delivery of that product to the buyer. There are many cases mentioned in the media or social networks where buyers on such sites complained that they paid but did not receive the product, so they were defrauded. The doctoral student sees here a real opportunity to implement security measures for online payments in advance, such as the introduction of an escrow system provided by the online platform so that the money is not sent directly to the seller but is temporarily detained in an escrow account by the online platform, to be returned to the seller after the buyer confirms the appropriate receipt of the product ordered.

Conversely, to protect the seller from sending the product but not collecting the money, the online platform will require the buyer first to pay the money to the online platform and then the seller delivers the product. Currently, there is no clearly defined and implemented security system (platforms offering such services even have a "disclaimer" by declining responsibility for the act of trade between the buyer and the seller) and therefore the doctoral student sees opportunity for further research and implementation of payment security measures for these second-hand online trading platforms.

INFORMAŢII PERSONALE

Marius Burcă

Aleea Stănilă nr. 5, Bl. H7, Sc. C, Ap. 57, Sector 3, București

0721856205

mariusburca@yahoo.com

Sex Male | Date of birth 09/11/1972 | Nationality Romanian

TARGET STUDIES

PhD in Management

WORK EXPERIENCE

From July 2015 to present

Marketing Manager/ Risk and Online Payments Auditor

SC Bet Zone SRL, brand “Fortuna”

- Create and implement the marketing strategy of the company
- Develop the Risk and Online Payments department
- Hire and train personnel

Sector online gambling

From Nov 2011 till July 2013

Project Manager

Sumup Limited (www.sumup.com)

- AML and Anti-Fraud compliance for online payments under Irish, German and UK legislations
- Create and implement procedures for AML (Anti-Money Laundering) and anti-fraud
- Supervise company payments

Sector: IT, online payments

From March 2007 till Feb 2012

Marketing Consultant

Earthquake Media

- General compliance for online gambling under Romanian legislation
- Create and implement marketing policies
- Supervise customer activity to prevent fraud and money laundering

Sector IT, online gambling

From Apr 2002 till July 2013

Administrator

Gamebookers Divertisment SRL

- General compliance for gambling activity under the License of the Ministry of Finance Romania
- Create and implement marketing strategy
- Implement anti-fraud and AML policies
- Hire and trains personnel
- Supervise the financial statements and company accounts

Sector gambling

EDUCATION

From 1999 till 2001

Master in International Business

Norwegian School of Economics and Business Administration, Bergen, Norvegia

- This is an MBA degree with focus on international Business

From 1991 till 1996

University degree

ASE Bucharest, Faculty of International Business

- 5-year curricula

COMPETENTE PERSONALE

Mother tongue: Romanian

Foreign languages

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C2	C2	C2	C2	C2
	Cambridge CPE, Grade B				
French	A1	A2	A1	A1	

Levels: A1/2: Basic user - B1/2: Independent user - C1/2: Proficient user
Common European Framework of Reference for Languages

Communication skills

- High communication skills acquired during personnel training

Management skills

- Leadership: I have been in charge with leading teams
- I have opened the branch of Sumup Limited in Amsteram
- I have created and run 2 companies in Romania

Skill acquired on the job

- Compliance in AML and anti-fraud
- Good understanding of probability theory

IT skills

- Good command of Microsoft Office™
- Worked with Adobe Fireworks
- Basic knowledge of HTML and CSS
- Basic knowledge of SQL

Driving license

- B category

OTHER INFORMATION

Memberships

- Affiliate membership (no. 674613) of Association of Certified Fraud Examiners, Houston, Texas

References

- Marine Jouaillec, former Legal adviser, SumUp Limited, mobile +33661489501, email marinejouaillec@gmail.com
- Michael Maerz, former Director of Sportsbetting, Party Gaming, mobile +35058009382, email maerzmichael@yahoo.com
- Piotr Blazewicz, former Regional Manager, Party Gaming, mobile +34654499653, email piotr.blazewicz@gmail.com

DATE: 06.12. 2017

SIGNATURE: