ROMÂNIA
JUDECĂTORIA BRĂILA
CALEA CĂLĂRAŞILOR NR 47
BRĂILA
SECŢIA CIVILĂ
Camera Sala 1 Judecatorie

Destinatar:
CINA LACT SRL
BRĂILA, Str. Şcolilor, bl. B15, et. parter judeţul BRĂILA

DOSARUL NR. 17883/196/2023
Materia: Civil
Stadiul procesual al dosarului: Fond
Obiectul dosarului: pretenţii

CITAŢIE
emisă la 10 Aprilie 2024

Stimată doamnă/Stimate domn,

Sunteţi chemat în această instanţă, camera Sala 1 Judecatorie, Complet c 4.civil, în data de 27 Noiembrie 2024, ora 11:00 în calitate de **reclamant**, în proces cu **BANCA COMERCIALĂ ROMÂNĂ SA - SUCURSALA BRĂILA** în calitate de pârât.

Cu copie întâmpinare, cu posibilitatea de a depune răspuns la acesta în termen de 10 zile de la comunicare.

Prin înmânarea citaţiei, sub semnătură de primire, personal ori prin reprezentant legal sau convenţional ori prin funcţionarul sau persoana însarcinată cu primirea corespondenţei pentru un termen de judecată, cel citat este prezumat că are în cunoştinţă şi termenele de judecată ulterioare aceluia pentru care citaţia i-a fost înmânată.

PARAFA ŞEFULUI INSTANŢEI
(ştampila)

Grefier,

Banca Comercială Română S.A.
Societate administrată în sistem dualist
www.bcr.ro

Şoseaua Orhideelor nr. 15D, Clădirea The Bridge 1, etajul 2, Sector 6, Bucureşti, cod poştal 060071

contact.center@bcr.ro
InfoBCR: *2227 apelabil din reţelele Vodafone, Orange, RCS, RDS, Telekom; + 4021.407.42.00, apelabil din orice reţea din România sau din străinătate

Înmatriculată la Registrul Comerţului: J40/90/1991
Înmatriculată la Registrul Instituţiilor de Credit: Nr. RB-PJR-40-008/18.02.1999

Cod Unic de Înregistrare: RO 361757
Capital Social: 1.625.341.625,40 lei
SWIFT: RNCB RO BU

Nr.DJ/i/440085/17.01.2023

De la: DIRECTIA JURIDICA

Catre: JUDECATORIA BRAILA
SECTIA CIVILA

Referitor: DOSAR NR. 17883/196/2023

Subscrisa Banca Comerciala Romana SA, cu sediul in Bucuresti, Şoseaua Orhideelor nr. 15 D, Clădirea The Bridge 1, etajul 2, Sector 6, Bucureşti, cod poştal 060071, in calitate de parata, in temeiul art. 205 C.proc.civ., formulam prezenta

INTAMPINARE

prin care solicitam respingerea actiunii ca nefondata pentru urmatoarele

MOTIVE:

Reclamanta a fost victima unui atac de phishing prin impersonarea paginii web George Login.

In urma investigatiei, s-a constatat existenta unei fraude externe de tip phishing, prin care clientii erau indrumati sa isi actualizeze datele personale prin accesarea/scanarea unui cod QR si introducerea unui cod de semnare tranzactie.

Astfel, in urma discutiei cu clientii pagubiti cat si pe baza datelor existente in Banca a fost identificat urmatorul modus operandi:

1) Clientii au incercat accesarea serviciului BCR de internet Banking - George, prin utilizarea motorului de cautare Google. Dupa afisarea de catre motorul de cautare a paginilor WEB, **clientii BCR au ales o pagina care nu este a BCR, un exemplu fiind https://loqln-bcrro.com - o pagina WEB folosita de persoane necunoscute pentru actiuni de phishing;**

2) Clientii au accesat unul din rezultate returnate de Google - Login George, in loc sa acceseze butonul de pe site-ul www.bcr.ro;

3) In pagina web falsa a aplicatiei George, clientilor li s-a solicitat sa isi actualizeze datele prin accesarea/scanarea unui cod QR sau introducerea unui cod de semnare tranzactie. Astfel, clientii BCR si-au introdus credentialele in respectiva pagina (datale de conectare si codurile de securitate generate de aplicatia eToken / Token) dand posibilitatea persoanelor care controlau pagina respectiva sa acceseze in numele clientului aplicatia reala George WEB si sa initieze transferuri in conturile acestora, in timp ce clientii BCR erau blocati in pagina de phishing asteptand sa acceseze aplicatia.

In acest fel, atacatorii au reusit sa acceseze fondurile clientilor BCR si sa efectueze transferuri neautorizate din conturile acestora catre conturi deschise la BCR sau alte banci din Romania sau strainatate.

Banca a solicitat reclamantei o descriere detaliata a evenimentelor petrecute in 04.10.2022, la momentul in care clientul a accesat contul George : cum a accesat platforma George (printr-un link primit pe email de actualizare date, prin Google, etc), ce s-a intamplat la logare, ce date i-au fost solicitate, ce date a introdus, daca i-a fost solicitata o actualizare de date, orice amanunt care poate face diferenta fata de o conectare normala in aplicatie.

In cazul reclamantei, conform celor declarate de clienta (e-mail atasat din data de 22 dec. 2022), contabila societatii, d-na Taflan Elena a accesat in data de 04.10.2022 George via Google, moment in care a primit mesajul specific dat de pagina de phishing.

„Subsemnata Taflan Elena, in calitate de responsabil economic la CINA LACT SRL, persoana responsabila cu operatiunile de cont curent ale societatii, care detin si datele de acces, referitor la accesul din data de 04.10.2022 la aplicatia de gestiune a contului societatii, declar urmatoarele:

In data de 04.10.2022 am accesat contul societatii CINA LACT SRL, prin google cu intentia de a lista extrasele de cont in vederea inregistrarii acestora in contabilitate.

Nu am initiat nici o plata deoarece nu aveam nimic de platit nici in euro si nici in lei.

Am listat extrasele in lei fara nici o problema.

Ulterior, la aceeasi data, am vrut sa accesez din nou contul pentru a lista extrasul in euro si nu am reusit deoarece imi aparea un mesaj precum ca momentan serviciul BCR este indisponibil.

Peste cateva zile am accesat din nou contul, prin intermediul internetului, cu intentia de a lista extrasul in euro, pentru a efectua inregistrarile in contabilitate. Cu aceasta ocazie am constatat plata sumei de 19.700 euro, plata pe care nu am initiat-o si nu am autorizat-o.

Aceasta situatie am adus-o la cunostinta administratorului societatii, dnul Mocanu Valentin.

Declar ca sunt singura persoana din cadrul societatii care accesez contul si care detine datele de acces.(s.n.)"

Suma de 19.700 EUR a fost transferata in contul unei persoane fizice Rotaru Petru, cont deschis tot in BCR, iar de acolo catre dealer-ul de cryptomonede Kraken.

BCR a trimis catre banca destinatara a platii solicitarea de retur plata pe motiv de frauda, dar fondurile erau deja retrase.

Relatiile contractuale dintre banca si clientii sai persoane juridice sunt guvernate de documentul denumit Termenii si Conditiile Generale de Afaceri, referitor la care, in orice document contractual sau de modificare a contractului, se precizeaza urmatoarele:

f. ca am inteles si acceptat in mod expres continutul prevederilor din TCGA, inclusiv dar fara a se limita la prevederile Cap I (in special Sectiunea C); Cap II (in special Sectiunea A Clauzele 2, 3 si 4 - teza finala; Sectiunea C Clauzele 4 si 5; Sectiunea D Clauzele 3, 6, 7, 8, 9, 23 si 25; Sectiunea F Clauzele 3, 5 si 6); Cap III (in special Sectiunea B Clauzele 4, 16, 24 si 26; Sectiunea C Clauzele 2, 4, 5, 6, 7, 9, 11, 12, 13 si 14; Sectiunea D Clauza 1; Sectiunea E Clauzele 1-6; Sectiunea F); Cap VI (in special Sectiunea A Clauzele 2 si 3; Sectiunea C Clauzele 1 - 3; Sectiunea D Clauzele 1 -3; Sectiunea E Clauzele 1 si 2), Sectiunea F (Anexa 7, partea II-clauza 3.27, partea III.2-clauza 4) din TCGA care se refera, printre altele, la limitarea raspunderii Bancii, modificarea si incetarea efectelor TCGA, suspendarea sau refuzarea executarii obligatiilor contractuale sau a operatiunilor si instructiunilor specifice, operarea compensarii conventionale, inchiderea conturilor, limitarea efectelor impreviziunii, raspunderea pentru situatiile de caz fortuit sau forta majora, posibilitatea de cesionare a documentatiei contractuale si aplicarea legii romane;

(a se vedea in Cererea de deschidere a Pachetului de produse si servicii BCR Succes, la capitolul V, pct. 2, lit. f).

Reclamanta a optat pentru luarea la cunostinta a prevederile TCGA de pe site-ul bancii (www.bcr.ro), asa cum se mentioneaza in Cererea de deschidere a Pachetului de produse si servicii BCR Succes nr. 1/29.12.2021, la art. V, pct. 2, lit. j):

j. ca am luat la cunostinta, am citit si acceptat in mod expres prevederile Termenilor si Conditiilor Generale de Afaceri pentru persoane juridice si persoane care desfasoara activitati independente impreuna cu toate anexele acestuia (astfel cum sunt afisate pe site-ul Bancii www.bcr.ro) (denumit Impreuna "TCGA"), al caror continut confirm ca mi-a fost furnizat prin accesarea site-ului www.bcr.ro si ca fac parte integranta cu prezentul Contract. Suplimentar confirm ca am luat la cunostinta, am citit si acceptat in mod expres prevederile specifice fiecarui produs si serviciu achizitionat conform prezentului Contract astfel cum sunt prevazute in anexele relevante la TCGA;

Reclamanta utilizeaza serviciul George (Digital Banking).

In speta, reclamanta a fost victima unui atac tip phishing - aceasta a accesat o pagina falsa de internet George BCR, in cadrul careia i-au fost solicitate datele personale bancare, precum si codurile de semnare generate de token, pe care clienta le-a oferit.

Cu datele obtinute astfel, atacatorii au accesat contul clientului si au ordonat o plata in valoare de 19.700 eur catre clientul ROTARU PETRU, cont RO28RNCB0175171040530003.

De aici, s-a efectuat o plata in valoare de 19695 EUR catre Kraken - un dealer de cryptomonede din Germania.

In urma mesajului de retur plata pe motiv de frauda trimis catre destinatarul platii a fost primit mesaj din partea bancii destinatare a platii prin care eram informati ca suma a fost deja retrasa si nu poate fi recuperata.

Prin urmare, tranzactia efectuata, contestata de catre reclamanta, a fost efectuata din neglijenta acesteia, aceasta furnizand datele cardului si elementele de securitate ale acestuia si divulgand elementele de confidentialitate.

Deci, tranzactia fiind autorizata prin credentialele reclamantei, banca nu are dreptul de a initia actiuni de recuperare a sumelor pentru acest tip de tranzactii, de la beneficiari ai platilor, plata fiind autorizata.

In conformitate cu TCGA cap. 5, punctul 5, „Suplimentar celor de mai sus, Clientul confirma si este de acord ca, atat Clientul cat si oricare din reprezentantii sai, persoane imputernicite (inclusiv Imputerniciti pe Cont si/sau Utilizatori, dupa caz) sau Delegati prin Documentatia Contractuala, au obligatia sa pastreze in siguranta si sa ia masuri de protejare a oricaror Elemente de Securitate, sa nu divulge Elementele de Securitate unor persoane neautorizate si/sau sa inregistreze Elementele de Securitate intr-o forma ce poate fi recunoscuta, sa nu instraineze Elementele de Securitate, sa se asigure ca PIN-ul Cardului este tastat la terminalul electronic (POS sau ATM), astfel incat acesta sa nu fie vazut de alte persoane, respectiv sa se asigure ca orice dispozitiv Token / Aplicatie e-Token BCR / Dispozitiv Extern / Cardul este utilizat doar de catre Utilizatori in acest sens.

In Anexa 7 - Termeni si conditii privind utilizarea serviciilor de Electronic Banking , pct. C., anexa la TCGA, se reglementeaza urmatoarele:

C.Conditii specifice de utilizare a Serviciului Internet Banking, Mobile Banking si Phone Banking

1. In cadrul Serviciului Internet Banking, Mobile Banking si Phone Banking, Detinatorul are posibilitatea de a beneficia de Servicii Bancare si functionalitati prin intermediul internetului sau al comunicarii telefonice. Accesul se face prin Nume de Utilizator si cod OTP si permite fara a se limita la: transferuri intra/interbancare in lei si valuta pentru toate tipurile de conturi bancare curente, cu executare in data curenta sau programate cu executare intr-o data din viitor (fara ciclicitate); Plati Programate cu ciclicitate (Standing Order); administrare limite proprii de tranzactionare; plati multiple constand in transmiterea de fisiere de plati intrabancare in lei si valuta si interbancare in lei, intr-un format agreat de Banca (operatiune indisponibila pentru Clientii PDAI), operatiuni de schimb valutar, contractarea, modificarea si inchiderea de Servicii Bancare sau administrarea anumitor date de contact ale Detinatorului. 2. Serviciul Internet Banking, Mobile Banking si Phone Banking are trei componente/canale, si anume: Internet Banking, Mobile Banking si Phone Banking. 3. Serviciile de Internet Banking si Mobile Banking permit Detinatorului, prin Utilizatorul Autorizat, efectuarea de tranzactii si obtinerea de informatii personalizate despre conturile bancare curente activate pentru aceste componente ale Serviciului Bancar. Operatiunile sunt initiate direct de catre Utilizatorul Autorizat, prin accesarea zonei dedicate de pe Pagina de Internet (in cazul Serviciului Internet Banking) sau prin accesarea aplicatiei de mobile banking pusa la dispozitie de catre Banca pe internet (in cazul Serviciului Mobile Banking).

2. Serviciul Internet Banking, Mobile Banking si Phone Banking are trei componente/canale, si anume: Internet Banking, Mobile Banking si Phone Banking.

3. Serviciile de Internet Banking si Mobile Banking permit Detinatorului, prin Utilizatorul Autorizat, efectuarea de tranzactii si obtinerea de informatii personalizate despre conturile bancare curente activate pentru aceste componente ale Serviciului Bancar. Operatiunile sunt initiate direct de catre Utilizatorul Autorizat, prin accesarea zonei dedicate de pe Pagina de Internet (in cazul Serviciului Internet Banking) sau prin accesarea aplicatiei de mobile banking pusa la dispozitie de catre Banca pe internet (in cazul Serviciului Mobile Banking).

Tranzactia a fost efectuata cu AUTENTIFICARE STRICTA, asa cum este definit in art. 5 alin. 1, pct. 4 din Legea nr. 209/2019 privind serviciile de plata si pentru modificarea unor acte normative:

„ 4. autentificarea stricta a clientilor - autentificare care se bazeaza pe utilizarea a doua sau mai multe elemente incluse in categoria cunostintelor detinute (ceva ce doar utilizatorul cunoaste), posesiei (ceva ce doar utilizatorul poseda) si inerentei (ceva ce reprezinta utilizatorul) care sunt independente, iar compromiterea unui element nu conduce la compromiterea fiabilitatii celorlalte elemente, si care sunt concepute in asa fel incat sa protejeze confidentialitatea datelor de autentificare;".

Potrivit art. 147 din Legea nr. 209/2019 privind serviciile de plata si pentru modificarea unor acte normative, „o operatiune de plata este considerata autorizata doar daca platitorul si-a exprimat consimtamantul pentru efectuarea operatiunii de plata".

In cazul de fata, procedura de autentificare a fost efectuata, inregistrata corect, introdusa in cont si nefiind afectata de nicio defectiune tehnica ori de alte deficiente ale serviciilor prestate de banca.

Conform TCGA cap.2, lit. D, pct.10, d), consimtamantul clientului pentru executarea operatiunii de plata transmise prin intermediul serviciilor internet banking se face prin introducerea codului DS (digital signiture) fiind codul unic generat de dispozitivul Token/ Aplicatia eToken BCR, conform instructiunilor specifice, cu ajutorul caruia Clientul isi exprima consimtamantul si autorizeaza operatiunile efectuate prin intermediul Serviciilor e-BCR, Internet Banking, Mobile Banking si Business 24 Banking BCR.

Limitarea raspunderii BCR - in situatia transmiterii de catre client a unor instructiuni prin intermediul Internet Banking si Mobile Banking, BCR nu este responsabila pentru executarea respectivelor Instructiuni, DACA ACESTEA AU FOST EMISE DE PERSOANE NEAUTORIZATE CARE AU CUNOSCUT PAROLELE DE ACCES SI ELEMENTELE DE SECURITATE SPECIFICE SAU AU FOST EMISE DE CATRE CLIENT FARA RESPECTAREA CERINTELOR TEHNICE PREVAZUTE IN CONVENTIILE RELEVANTE.

Prin urmare, Banca nu este obligata sa despagubeasca clientul, deoarece conform art. 179 din Legea nr. 209/2019, "Platitorul suporta toate pierderile legate de orice operatiune de plata neautorizata daca aceste pierderi au fost cauzate de platitor in urma fraudei sau a nerespectarii, intentionate sau din neglijenta grava, a uneia sau a mai multor obligatii prevazute la art. 166".

"Art. 166:

(1) Utilizatorul serviciilor de plata care foloseste un instrument de plata are urmatoarele obligatii:

a) sa utilizeze instrumentul de plata in conformitate cu clauzele care reglementeaza emiterea si utilizarea acestuia;

b) sa notifice prestatorul de servicii de plata sau entitatea desemnata de acesta, fara intarziere nejustificata, de indata ce ia cunostinta de pierderea, furtul, folosirea fara drept a instrumentului sau de plata sau de orice alta utilizare neautorizata a acestuia.

(2) In scopul prevazut la alin. (1) lit. a), de indata ce utilizatorul serviciilor de plata primeste un instrument de plata, acesta ia toate masurile rezonabile pentru a pastra in siguranta elementele de securitate personalizate.

Art. 179:

(1) Prin exceptie de la prevederile art. 173-176, platitorul poate fi obligat, pana la un cuantum de cel mult 30 euro sau echivalentul in lei, sa suporte consecintele financiare legate de orice operatiune de plata neautorizata care rezulta din utilizarea unui instrument de plata pierdut sau furat sau din folosirea fara drept a acestuia, in cazul in care platitorul nu a actionat in mod fraudulos si nici nu si-a incalcat, cu intentie, obligatiile ce ii revin in temeiul art. 166. Acest alineat nu se aplica in situatiile prevazute la art. 177.

(2) Platitorul suporta toate pierderile legate de orice operatiune de plata neautorizata daca aceste pierderi au fost cauzate de platitor in urma fraudei sau a nerespectarii, intentionate sau din neglijenta grava, a uneia sau a mai multor obligatii prevazute la art. 166. In astfel de cazuri, suma de cel mult 30 euro sau echivalentul in lei al acestei sume nu se aplica.

(3) Evaluarea raspunderii platitorului se face tinand cont, in special, de natura elementelor de securitate personalizate ale instrumentului de plata si de situatiile in care acesta a fost pierdut, furat sau folosit fara drept.."

In concluzie, solicitam sa constatati ca pierderea suferita de reclamanta se datoreaza neglijentei sale grave intrucat a divulgat elementele de securitate personalizate.

Banca Nationala a Romaniei a publicat pe site-ul sau un comunicat si un studiu (link https://www.bnr.ro/Fraude-21235.aspx) prin care atrage atentia asupra noilor tipologii de fraude in domeniul platilor care vizeaza instrumentele de plata electronica de tip card, internet banking sau mobile banking.

In studiu, s-a retinut ca o problema deosebit de importanta este legata de modul in care sunt suportate pierderile in cazul operatiunilor de plata efectuate in mod fraudulos, ca urmare a unor atacuri de tip phishing.

Acesta problema si-a gasit raspunsul la nivel european in cadrul legislativ care reglementeaza serviciile de plata, respectiv Directiva revizuita privind serviciile de plata in cadrul pietei interne, ce a fost transpusa in legislatia nationala prin Legea nr. 209/2019 privind serviciile de plata si pentru modificarea unor acte normative.

Principiul juridic de baza urmarit de legislatie este ca raspunderea patrimoniala revine celui aflat in culpa, respectiv celui care nu si-a indeplinit obligatiile ce ii reveneau conform reglementarilor in vigoare si a contractelor/conventiilor incheiate intre utilizatorul si prestatorul serviciilor de plati.

Prevederile legislative relevante pentru aceasta problematica se regasesc in cuprinsul Legii nr. 209/2019, la sectiunea a 6-a „Obligatiile partilor cu privire la instrumentele de plata si la elementele de securitate personalizate" si la sectiunea a 9-a „Raspunderea pentru operatiunile de plata neautorizate".

Din analiza textului de lege, se disting mai multe situatii, dupa cum urmeaza:

1. Daca operatiunile de plata contestate au fost efectuate fara ca prestatorul serviciilor de plata (banca emitenta) sa fi aplicat procedura de autorizare stricta a clientului, atunci banca emitenta este raspunzatoare si suporta prejudiciul, conform art. 177 lit. d) din lege;

2. In cazul in care operatiunile de plata contestate au fost efectuate prin aplicarea procedurii de autentificare stricta a clientului – in aceasta situatie, legislatia instituie o prezumtie legala ca tranzactia provine de la titularul legitim al instrumentului de plata in cauza sau ca acesta a transmis elementele de securitate personalizate unor terte persoane si, ca atare, prin faptul ca nu si-a indeplinit obligatiile de pastrare in siguranta a informatiilor respective, este in culpa si suporta prejudiciul (a se vedea in acest sens prevederile art. 166 alin. 2, coroborate cu cele ale art. 177 lit. d si ale art. 179 alin. 2 din Legea nr. 209/2019);

3. In situatia in care operatiunile de plata contestate au fost efectuate dupa ce clientul a notificat banca sa despre pierderea, furtul, folosirea fara drept a instrumentului sau de plata sau de orice alta utilizare neautorizata a acestuia, atunci banca emitenta este raspunzatoare si suporta prejudiciul, indiferent daca a aplicat sau nu procedura de autentificare stricta a clientilor (a se vedea prevederile art. 166 alin. 1 lit. a, coroborate cu cele ale art. 177 lit. c din Legea nr. 209/2019).

Autentificarea stricta a clientilor este o procedura reglementata la nivel european, menita sa asigure un grad sporit de securitate in cazul operatiunilor de plata electronice, prin prevenirea accesului neautorizat la conturile utilizatorilor si a fraudelor aferente tranzactiilor efectuate in mediul online. Dupa cum reiese din insasi denumirea sa, rolul acestei proceduri este de a confirma identitatea persoanei care initiaza si autorizeaza operatiunile de plata, respectiv de a garanta ca acestea sunt efectuate doar de titularul instrumentului de plata.

Din punct de vedere practic, autentificarea stricta a clientilor presupune folosirea a cel putin doua elemente de securitate (factori de autentificare), din categorii diferite, categorii ce sunt prezentate mai jos:

1. categoria „elemente de cunoastere" – informatii pe care doar titularul instrumentului de plata le cunoaste, cum ar fi: codul PIN sau o parola (de obicei, numita „parola statica", pentru ca este valabila pentru o perioada mai lunga de timp);

2. categoria „elemente de posesie" – elemente pe care doar titularul instrumentului de plata le detine, spre exemplu un dispozitiv de incredere (cum ar fi un telefon mobil sau o tableta), dispozitiv care a fost agreat in prealabil cu banca pentru transmiterea elementelor de securitate personalizate clientului sau. In acest caz, banca trimite prin SMS, pe numarul de telefon convenit

anterior, un cod pe care clientul il va folosi in procesul de autentificare (codul/parola respectiva este numita „parola dinamica" sau „one time password", fiind generata in mod automat de catre sistemul bancii pentru fiecare operatiune in parte). O alta varianta este folosirea unui dispozitiv de tip token care va genera un cod de autentificare. La randul sau, token-ul poate fi de tip hardware, respectiv un dispozitiv fizic pe care banca il pune la dispozitia exclusiva a clientului, sau de tip software, respectiv o aplicatie ce se instaleaza pe telefon/tableta, dupa ce, in prealabil, s-a aplicat o procedura de autentificare stricta a clientului.

3. categoria „elemente de inerenta" – ceva ce „clientul este", in aceasta categorie intrand recunoasterea clientului pe baza amprentei digitale, identificarii faciale sau a altor elemente de biometrie.

Toate aceste aspecte legate de procedura de autentificare stricta a clientilor sunt reglementate detaliat in cuprinsul Regulamentului delegat (UE) nr. 2018/389 de completare a Directivei (UE) 2015/2366 a Parlamentului European si a Consiliului cu privire la standardele tehnice de reglementare pentru autentificarea stricta a clientilor si standardele deschise, comune si sigure de comunicare (link https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX%3A32018R0389).

Din punct de vedere tehnic, procedura de autentificare stricta a clientului este foarte sigura si nu poate fi compromisa de catre atacatori daca titularul instrumentului de plata nu face greseala de a le comunica acestora elementele sale de securitate personalizate.

Avand in vedere cele de mai sus, solicitam sa retineti ca reclamanta, prin transmiterea elementelor de securitate persoanalizate, nu si-a indeplinit obligatia de a pastra in siguranta informatiile respective, si ca este in culpa in situatia producerii fraudei, iar prestatorul de servicii de plata nu poate fi obigat sa suporte eventualul prejudiciu.

Solicitam proba cu inscrisuri, cat si orice alte probe a caror necesitate rezulta din dezbateri.

Depunem actele invocate, TCGA si anexe, extrase de cont.

Sef departament,

Raul Dabija

Petru-Raul Dabija

Digitally signed by Petru-Raul Dabija
Date: 2024.01.18 14:13:41 +02'00'

BANCA COMERCIALA ROMANA BCR DIRECTIA JURIDICA

Supervizor,

Valentin Vidrighin

Valentin Vidrighin

Digitally signed by Valentin Vidrighin
Date: 2024.01.18 14:11:40 +02'00'

Consilier juridic,

Constanta Voicu

Constanta Voicu BCR

From: Sorin Catalin Enache BCR
Sent: Thursday, December 22, 2022 2:25 PM
To: Iulian Abdula BCR
Subject: FW: RCR00617255 CINA LACT SRL - suspiciune frauda transfer eur BCR-BCR

Buna ziua,

Am primit din partea clientului precizarile de mai jos.

Multumesc,

From: Valentin Mocanu <valentinmocanu68@yahoo.com>
Sent: Thursday, December 22, 2022 1:59 PM
To: Sorin Catalin Enache BCR <SorinCatalin.Enache@bcr.ro>
Subject: Re: RCR00617255 CINA LACT SRL - suspiciune frauda transfer eur BCR-BCR

Subsemnata Taflan Elena,in calitate de responsabil economic la CINA LACT SRL, persoana responsabila cu operatiunile de cont curent ale societatii, care detin si datele de acces, referitor la accesul din data de 04.10.2022 la aplicatia de gestiune a contului societatii, declar urmatoarele:

In data de 04.10.2022 am accesat contul societatii CINA LACT SRL,prin google cu intentia de a lista extrasele de cont in vederea inregistrarii acestora in contabilitate.

Nu am initiat nici o plata deoarece nu aveam nimic de platit nici in euro si nici in lei.

Am listat extrasele in lei fara nici o problema.

Ulterior, la aceeasi data, am vrut sa accesez din nou contul pentru a lista extrasul in euro si nu am reusit deoarece imi aparea un mesaj precum ca momentan serviciul BCR este indisponibil.

Peste cateva zile am accesat din nou contul, prin intermediul internetului, cu intentia de a lista extrasul in euro, pentru a efectua inregistrarile in contabilitate. Cu aceasta ocazie am constatat plata sumei de 19.700 euro, plata pe care nu am initiat-o si nu am autorizat-o.

Aceasta situatie am adus-o la cunostinta administratorului societatii, dnul Mocanu Valentin.

Declar ca sunt singura persoana din cadrul societatii care accesez contul si care detine datele de acces.

On Wednesday, December 21, 2022 at 12:09:37 PM GMT+2, Sorin Catalin Enache BCR <sorincatalin.enache@bcr.ro> wrote:

Avem nevoie din partea clientului de o descriere detaliata a evenimentelor petrecute in 04.10.2022, la momentul in care clientul a accesat contul George : cum a accesat platforma George (printr-un link primit pe email de actualizare date, prin Google, etc), ce s-a intamplat la logare, ce date i-au fost solicitate, ce date a introdus, daca i-a fost solicitata o actuializare de date, orice amanunt care poate face diferenta fata de o conectare normala in aplicatie.

Multumesc

O zi placuta