BNR a primit anul trecut cu 23% mai sesizari privind serviciile de plata utilizate

Banca Nationala a României a receptionat, în 2023, cu aproximativ 23% mai multe sesizari prin care sunt reclamate si/sau contestate anumite aspecte legate de serviciile de plata utilizate, dintre care 57% au vizat aspecte privind scenarii de frauda bazate pe tipologii de manipulare a platitorului si spete de phishing, potrivit raportului anual al bancii centrale.

"Pe parcursul anului 2023, raportat la anul precedent, BNR a receptionat cu aproximativ 23% mai multe sesizari prin care sunt reclamate si/sau contestate anumite aspecte legate de serviciile de plata utilizate. Astfel, dintre acestea: 57% au vizat aspecte privind scenarii de frauda bazate pe tipologii de manipulare a platitorului si spete de phishing; 18% au vizat solicitari privind decontarea si procesarea operatiunilor de plata (operatiuni de plata dublate, timpul necorespunzator de decontare a operatiunilor de plata în valuta, operatiuni de tip charge-back, operatiuni de plata neprocesate datorita nefurnizarii documentelor justificative); 5% au prezentat probleme privind operatiunile de retragere si depunere de numerar la ATM/MFM (bancomate multifunctionale Multi-Function Machine); 4% au fost în legatura cu aspecte privind serviciile de open banking; 4% au vizat operatiuni de plata contestate de utilizatori ai serviciilor de plata (eroare POS, friendly/family fraud); 12% au vizat alte aspecte (solicitari de informatii inclusiv cu privire la aplicarea procedurii de autentificare stricta a clientilor, semnalarea deficientelor/nefunctionarii instrumentelor de plata electronica cu acces la distanta de tip internet/mobile banking, alte solicitari de informatii)", se mentioneaza în document.

Conform BNR, cele mai des întâlnite tipare de frauda sunt: ingineriile sociale - scopul este obtinerea de catre fraudatori a elementelor de securitate personalizate aferente instrumentelor de plata (coduri de acces, datele cardului, coduri de autentificare) si utilizarea acestora în vederea initierii, de catre acestia, de operatiuni de plata frauduloase; fraudele cu scop de investitii (criptoactive) - fraudatorii care pretind ca actioneaza în nume propriu sau sunt angajati la companii cu renume în domeniu contacteaza diverse persoane pentru a le propune sa faca investitii si reusesc sa-i determine sa ofere date sensibile privind platile (datele cardului, parole de acces la aplicatiile de plata, codurile OTP primite prin SMS etc.) sau sa instaleze pe telefonul acestora aplicatii care permit accesul la dispozitivul victimelor de la distanta, sub pretextul obtinerii unor câstiguri mari cu investitii mici sau retragerii profitului înregistrat ca urmare a activitatii de tranzactionare pe diverse platforme de criptoactive.

De asemenea, în unele cazuri, acestia au manipulat persoanele contactate, determinându-le sa obtina o linie de credit, scopul final fiind transferarea fondurilor astfel obtinute în conturile proprii sau ale persoanelor pe care le controlau.

În raport se precizeaza ca tiparele de frauda sunt într-o continua evolutie, fraudatorii cautând permanent variatiuni ale metodelor existente sau noi metode de fraudare, unele bazate pe tehnologie. Deep-fake este una dintre metodele noi de fraudare întâlnite la nivel international si reprezinta orice continut falsificat de tip imagine, audio si/sau video realizat cu ajutorul tehnologiei AI (inteligenta artificiala), astfel încât sa creeze aparenta ca o persoana a spus sau a facut lucruri pentru care nu si-a dat consimtamântul, care, în realitate, nu au fost spuse sau facute de acea persoana, scopul final fiind obtinerea de câstiguri financiare.

BNR sustine ca monitorizeaza continuu evolutia fraudelor si a tiparelor de frauda si emite recomandari si îndrumari prestatorilor de servicii de plata privind masurile de securitate suplimentare care pot fi implementate în vederea identificarii si evitarii fraudelor.

Printre recomandarile adresate prestatorilor de servicii de plata de catre BNR, în cursul anului 2023, se regasesc: îmbunatatirea sistemelor de monitorizare a tranzactiilor utilizate de catre prestatorii de servicii de plata astfel încât acestea sa permita identificarea si blocarea operatiunilor de plata frauduloase în timp real; aderarea

prestatorilor serviciilor de plata la Serviciul Afisare Nume Beneficiar (SANB) pus la dispozitie de catre Transfond SA; îmbunatatirea fluxurilor de înrolare în aplicatiile de plata precum si a fluxurilor de înrolare a cardurilor în diverse aplicatii de plata.