Part of the ProCredit Group

ProCredit Bank

# Siguranța cardului, online și offline

Pentru a evita potențialele fraude, vă încurajăm să respectați regulile de mai jos:

## Ameninţări privind plăţile cu cardul

### Păstrați-vă cardul în siguranță

Păstraţi cardul bancar cu aceeaşi grijă cu care păstraţi şi actul de identitate!

### Păstrați-vă PIN-ul în siguranță

Asigurați confidențialitatea numărului personal de identificare a cardului (PIN)!

Din motive de Securitate, codul PIN nu trebuie stocat pe niciun suport electronic sau de hârtie și nu trebuie divulgate nimănui!

### Alegeți un PIN sigur

În cazul în care alegeți să vă creați un nou PIN sau să îl schimbați pe cel care v-a fost furnizat de către Bancă, evitați alegerile evidente cum ar fi data nașterii dumneavoastră sau a membrilor familiei.

Part of the ProCredit Group

ProCredit Bank

La efectuarea unei tranzacţii cu cardul pe internet sunt necesare următoarele date:

1. Tipul cardului: Visa, MasterCard, etc
2. Nume titularului cardului (aşa cum apare pe card)
3. Numărul cardului (cele 4 grupuri a câte 4 cifre aflate pe card)
4. Data expirării cardului (se găseşte sub numărul cardului şi este de forma ll/aa
5. CVV2 (Card Verification Value – nume utilizat de Visa) sau CVC2 (Card Verification Code – nume utilizat de MasterCard). Acesta este un cod de siguranţă format din 3 cifre şi este tipărit pe verso-ul cardului. Mai poate fi întâlnit pe Internet şi sub denumiri cum ar fi Card Security Code/Verification Code etc.
6. Parola sau codul OTP pentru tranzacţii prin sistemul “3D Secure” (Verified by Visa, sau Mastercard Securecode). Parola 3D-Secure sau codul unic OTP sunt elemente de siguranţă, de antifrauda, dezvoltate de VISA şi MasterCard. Folosirea acestui sistem asigură creşterea securităţii tranzacţiilor online.

Part of the ProCredit Group

ProCredit Bank

## Avantajele 3D Secure

Reducerea riscului de fraudă datorită faptului că doar persoana care cunoaşte parola 3D Secure, sau care cunoaşte codul OTP creat unic pentru acea tranzacţie 3D Secure (şi primit prin SMS, token sau alte canale), poate tranzacţiona online pe site-uri care folosesc acest sistem antifraudă.

Dacă datele cardului dumneavoastră înrolat în 3D Secure sunt folosite fraudulos de către o terţă parte pentru a comanda pe site-ul unui comerciant care nu foloseşte acest sistem de protecţie, veţi avea câştig de cauză la disputarea sumei aferente tranzacţiei.

# Atenție!

Nu răspundeţi niciodată e-mailurilor care par a fi trimise de banca emitentă a cardului, în care vă sunt solicitate datele sensibile ale cardului (număr card, data expirării, codul CVV2/CVC2, parola 3D Secure sau codul PIN) sub pretextul unor verificări, modificări, premii, colectării de informaţii pentru respectarea unor modificări legislative etc.

Atunci când efectuaţi cumpărături online, încercaţi să achiziţionaţi de la comercianţi cunoscuţi, care se bucura de o bună reputaţie.