AMERICAN EXPRESS

Politica Operațională cu Privire la Securitatea Datelor (DSOP)

AMERICAN EXPRESS

Rezumatul Modificărilor în DSOP

Pictograme

Actualizările importante sunt enumerate în Tabelul cu Rezumatul Modificărilor și, de asemenea, sunt indicate în *DSOP* cu o bară pentru modificare. O bară pentru modificare este o linie verticală, de regulă plasată în marginea stângă, care identifică textul adăugat sau revizuit. Numai modificările substanțiale din *DSOP* care pot afecta procedurile operaționale ale Comerciantului sunt indicate cu o bară pentru modificare, așa cum se observă în marginea stângă.

Textul eliminat este evidențiat cu pictograma coșului de gunoi în marginea apropiată oricărei ștergeri semnificative de text, inclusiv secțiuni, tabele, paragrafe, note și liste cu buline. Textul eliminat este indicat în acest Rezumat al Modificărilor prin numerele de secțiune din publicația anterioară pentru a evita confuzia.

Liniile albastre de lângă paragrafe indică informații cu specific regional.

Tabelul cu Rezumatul Modificărilor

Actualizările importante sunt enumerate în tabelul următor și, de asemenea, sunt indicate în *DSOP* cu o bară pentru modificare.

Secțiunea/Subsecțiunea	Descrierea Modificării
Nu există modificări pentru această versiune.	

Secțiunea 1 Introducere în DSOP și Standardele pentru Protecție

În calitate de lider în domeniul protecției consumatorilor, American Express s-a angajat pe termen lung să protejeze Datele personale ale Titularilor Cardurilor sale și Datele de Autentificare Sensibile, asigurându-se că acestea sunt păstrate în siguranță.

Datele compromise influențează în mod negativ consumatorii, Comercianții, Furnizorii de Servicii și emitenții de carduri. Chiar și un singur incident poate prejudicia grav reputația unei companii și poate afecta capacitatea acesteia de a-și desfășura activitatea în mod eficient. Combaterea acestei amenințări prin implementarea politicilor de operare privind securitatea poate contribui la sporirea încrederii clienților, la creșterea rentabilității și la consolidarea reputației companiei.

American Express este conștient de faptul că Furnizorii săi de Servicii și Comercianții (denumiți colectiv, Dvs.) împărtășesc preocuparea sa și solicită, ca parte a responsabilității acestora, ca **dvs.** să respectați prevederile privind securitatea datelor prin manifestarea propriului acord pentru acceptarea (în cazul Comercianților) sau procesarea (în cazul Furnizorilor de Servicii) a Cardului American Express® (fiecare dintre aceștia manifestând propriul **Acord**) și pentru această Politică Operațională cu privire la Securitatea Datelor (DSOP), pe care este posibil ca noi să o modificăm periodic. Aceste cerințe se aplică tuturor echipamentelor, sistemelor și rețelelor (și componentelor acestora) pe care sunt stocate sau prin care sunt procesate sau transmise Cheile de Criptare, Datele Titularilor Cardurilor sau Datele Sensibile de Autentificare (sau o combinație a acestora).

Termenii cu majusculă folosiți dar nedefiniți în acest document au semnificațiile atribuite acestora în glosarul disponibil la sfârșitul acestui document.

Politica Operațională cu Privire la Securitatea Datelor (DSOP) este o serie de cerințe cuprinzătoare care au rolul de a proteja Datele Contului în situații în care respectivele date sunt stocate, procesate sau transmise.

American Express solicită ca toți Comercianții și Furnizorii de Servicii să respecte Payment Card Industry Data Security Standard (PCI DSS). Pe baza respectivei cerințe, dvs. trebuie să acționați sau să determinați Părțile Interesate să acționeze după cum urmează:

- Să păstreze Datele Titularului Cardului doar pentru facilitarea Tranzacțiilor cu Cardul American Express în conformitate cu cerințele Acordului.
- Să respecte Cerințele actuale PCI DSS și alte Cerințe PCI Security Standards Council (PCI-SSC) aplicabile prelucrării, stocării sau transmiterii de către Dvs. a Cheilor de Criptare, Datelor Titularului Cardului sau a Datelor Sensibile de Autentificare nu mai târziu de data intrării în vigoare a implementării respectivei versiuni a cerinței aplicabile.
- Să se asigure că se utilizează produse aprobate PCI când se implementează sau se înlocuiește tehnologia pentru a stoca, procesa sau transmite date.

Dvs. trebuie să protejați toate înregistrările privind Debitările American Express și înregistrările de Credite păstrate în temeiul Acordului în conformitate cu aceste dispoziții privind securitatea datelor; aceste înregistrări trebuie utilizate numai în scopul Acordului și trebuie protejate în mod corespunzător. Dvs. sunteți răspunzător din punct de vedere financiar și nu numai față de American Express pentru asigurarea respectării de către Părțile Interesate a acestor prevederi privind securitatea datelor (altele decât cele care demonstrează conformitatea Părților Interesate cu această politică conform Secțiunea 2, „Programul de Conformitate PCI DSS (Validarea Periodică Importantă a Sistemelor Dvs.)”, cu excepția unor prevederi contrare din respectiva secțiune). Detaliile legate de standardele PCI și de modul de respectare a cerințelor respective se regăsesc pe www.pcisecuritystandards.org.

Secțiunea 2 Programul de Conformitate PCI DSS (Validarea Periodică Importantă a Sistemelor Dvs.)

Trebuie să urmați acțiunile de mai jos pentru a valida anual și la fiecare 90 de zile conform PCI DSS și potrivit descrierii de mai jos, starea echipamentului dvs., a sistemelor dvs. și/sau a rețelelor dvs. (și a componentelor lor)

și ale Francizaților dvs., pe care sunt păstrate, procesate sau transmise datele Titularilor Cardurilor sau Datele Sensibile de Autentificare.

Este necesară parcurgerea a patru acțiuni pentru efectuarea validării complete:

- Acțiune 1: Participarea la Programul de Conformitate PCI al American Express în temeiul acestei politici.
- Acțiune 2: Înțelegerea Nivelului Dvs. de Comerciant/Furnizor de Servicii și a Cerințelor Dvs. de Documentație de Validare.
- Acțiune 3: Completarea Documentației de Validare pe care Dvs. trebuie să o trimiteți către American Express.
- Acțiune 4: Trimiterea Documentației de Validare către American Express în termenul stabilit.

Acțiune 1: Participarea la Programul de Conformitate al American Express în temeiul acestei Politici

Comercianții de Nivel 1, Comercianții de Nivel 2 și toți Furnizorii de Servicii, conform descrierii de mai jos, trebuie să participe la Program conform acestei politici. American Express poate desemna, la propria sa discreție, Comercianți de Nivel 3 și Nivel 4 care să participe la Program conform acestei politici.

Comercianții și Furnizorii de Servicii care au obligativitatea de a participa la Program trebuie să se înscrie în Portalul furnizat de Administratorul Programului selectat de American Express, în intervalele de timp prevăzute.

- Trebuie să acceptați toți termenii și condițiile rezonabile asociate cu utilizarea Portalului.
- Trebuie să alocați și să precizați informații exacte pentru cel puțin o persoană de contact pentru securitatea datelor în cadrul Portalului. Informațiile solicitate includ:
  - Numele complet
  - Adresa de e-mail
  - Numărul de telefon
  - Adresa de corespondență fizică
- Când informațiile se modifică, trebuie să precizați informații de contact noi sau actualizate pentru persoana de contact alocată pentru securitatea datelor în cadrul Portalului.
- Trebuie să vă asigurați că v-ați actualizat sistemele pentru a permite servicii de comunicații de la domeniul desemnat al Portalului.

În cazul în care dvs. nu furnizați sau nu mențineți la zi astfel de informații ale persoanei de contact pentru securitatea datelor sau nu permiteți comunicațiile prin e-mail, nu vor fi afectate drepturile noastre de a evalua taxele.

Acțiune 2: Înțelegerea Nivelului Dvs. de Comerciant/Furnizor de Servicii și a Cerințelor Dvs. de Documentație de Validare

Există patru Niveluri pentru Comercianți și două Niveluri pentru Furnizorii de Servicii bazate pe volumul dvs. de Tranzacții cu Carduri American Express.

- În cazul Comercianților, acesta este volumul prezentat de Unitățile lor care rulează până la cel mai înalt nivel de cont Comerciant American Express.*
- Pentru Furnizorii de Servicii, aceasta este suma volumelor prezentate de Furnizorul de Servicii și de Furnizorul de Servicii Entități cărora le furnizați servicii.

Plățile în scop de business (BIP) nu sunt incluse în volumul Tranzacțiilor efectuate cu Carduri American Express pentru determinarea Nivelului de Comerciant și a cerințelor de validare. Vă veți încadra în unul dintre Nivelurile de Comerciant specificate în Tabelul A-1: Niveluri de Comercianți și Furnizori de Servicii.

* În cazul Francizorilor, acesta include volumul de la Unitățile Francizaților lor. Francizorii care mandatează Francizații să utilizeze un anumit Sistem pentru Punctele de Vânzare (POS) sau un anumit Furnizor de Servicii trebuie, de asemenea, să furnizeze documentația de validare pentru respectivii Francizați.

Tabelul A-1: Niveluri de Comercianți și Furnizori de Servicii

Nivel de Furnizor Comerciant	Tranzacții American Express anuale
Comerciant Nivelul 1	Peste 2,5 milioane de Tranzacții cu Carduri American Express pe an; sau orice alt Comerciant pe care American Express, din alte motive, îl consideră a fi de Nivelul 1.
Comerciant Nivelul 2	Între 50.000 și mai puțin de 2,5 milioane de Tranzacții cu Carduri American Express pe an.
Comerciant Nivelul 3	Între 10.000 și mai puțin de 50.000 de Tranzacții cu Carduri American Express pe an.
Comerciant Nivelul 4	Mai puțin de 10.000 de Tranzacții cu Carduri American Express pe an.
Nivel de Furnizor de Servicii	**Tranzacții American Express anuale**
Furnizor de Servicii Nivelul 1	Peste 2,5 milioane de Tranzacții cu Carduri American Express pe an; sau orice alt Furnizor de Servicii pe care American Express, din alte motive, îl consideră a fi de Nivelul 1.
Furnizor de Servicii Nivelul 2	Mai puțin de 2,5 milioane de Tranzacții cu Carduri American Express pe an; sau orice alt Furnizor de servicii pe care American Express nu îl consideră a fi de Nivelul 1.

Cerințe privind Documentația de Validare a Comercianților

Comercianții (nu Furnizorii de Servicii) au patru clasificări de Nivel de Comerciant posibile. După determinarea nivelului Comerciantului din Tabelul A-1: Niveluri de Comercianți și Furnizori de Servicii (vezi mai sus), consultați Tabelul A-2: Documentația de Validare a Comercianților pentru a determina cerințele documentației de validare.

Tabelul A-2: Documentația de Validare a Comercianților

Nivel Comerciant/ Tranzacții Anuale American Express	Raport privind Conformitatea și Atestarea Conformității (ROC AOC)	Chestionar de autoevaluare privind Atestarea Conformității (SAQ AOC) ȘI Scanarea Trimestrială a Vulnerabilității Rețelei Externe (Scanare)	Atestare pentru Programul de Îmbunătățire a Tehnologiei cu Privire la Securitate (STEP) pentru Comercianții eligibili
Nivelul 1/ Peste 2,5 milioane	Obligatoriu	Nu se aplică	Opțional cu aprobare de la American Express (înlocuiește ROC)
Nivelul 2/ Între 50.000 și mai puțin de 2,5 milioane	Opțional	SAQ AOC obligatoriu (cu excepția cazului în care se transmite un ROC AOC); scanare obligatorie la anumite tipuri SAQ	Opțional cu aprobare de la American Express* (înlocuiește SAQ și scanarea rețelei sau ROC)
Nivelul 3**/ Între 10.000 și mai puțin de 50.000	Opțional	SAQ AOC opțional (obligatoriu la solicitarea American Express); scanare obligatorie pentru anumite tipuri de SAQ	Opțional cu aprobare de la American Express* (înlocuiește SAQ și scanarea rețelei sau ROC)
Nivelul 4**/ Mai puțin de 10.000	Opțional	SAQ AOC opțional (obligatoriu la solicitarea American Express); scanare obligatorie pentru anumite tipuri de SAQ	Opțional cu aprobare de la American Express* (înlocuiește SAQ și scanarea rețelei sau ROC)

* **Notă:** Echipa PCI American Express va verifica solicitarea și eligibilitatea și va confirma dacă vă calificați în Programul STEP. Contactați-vă Managerul de Clienți și/sau AXPPCIComplianceProgram@aexp.com pentru a verifica eligibilitatea.

**Pentru evitarea neclarităților, Comercianții de Nivel 3 și Nivel 4 nu trebuie să trimită Documentația de Validare decât la solicitarea American Express, însă trebuie să respecte și își asumă răspunderea pentru toate celelalte prevederi ale acestei Politici Operaționale cu Privire la Securitatea Datelor.

American Express își rezervă dreptul de a verifica dacă Documentația de Validare PCI este completă, exactă și adecvată. American Express vă poate solicita să furnizați documente justificative suplimentare pentru evaluarea în acest scop. În plus, American Express are dreptul de a vă solicita să angajați un Evaluator de Securitate Calificat (QSA) sau un Investigator de Fraudă PCI (PFI) aprobat de PCI Security Standards Council.

Cerințe privind Documentația de Validare a Furnizorilor de Servicii

Furnizorii de Servicii (nu Comercianții) au două clasificări de Nivel posibile. După determinarea nivelului Furnizorului de Servicii din Tabelul A-1: Niveluri de Comercianți și Furnizori de Servicii (vezi mai sus), consultați Tabelul A-3: Documentația de Validare a Furnizorilor de Servicii pentru a determina cerințele documentației de validare.

Furnizorii de Servicii nu sunt eligibili pentru Programul de Îmbunătățire a Tehnologiei cu privire la Securitate.

Tabelul A-3: Documentația de Validare a Furnizorilor de Servicii

Nivel	Documentație de Validare	Cerință
1	Raport Anual privind Conformitatea și Atestarea Conformității (ROC AOC)	Obligatoriu
2	SAQ D Anual (Furnizor de Servicii) și Scanare Trimestrială a Rețelei sau Raport Anual privind Conformitatea și Atestarea Conformității (ROC AOC), dacă se preferă	Obligatoriu

Se recomandă ca Furnizorii de Servicii să respecte și Validarea Suplimentară a Entităților Desemnate de PCI.

Programul de Îmbunătățire a Tehnologiei cu Privire la Securitate (STEP)

Comercianții care îndeplinesc cerințele PCI DSS pot aplica, de asemenea, pentru STEP al American Express dacă utilizează anumite tehnologii de securitate suplimentare în mediile de procesare a Cardurilor. STEP se aplică numai în cazul în care Comerciantul nu a înregistrat un Incident de Date în ultimele 12 luni și dacă 75% dintre Tranzacțiile cu Cardul ale Comerciantului sunt efectuate utilizând o combinație a următoarelor opțiuni de securitate optimizată:

- **Tehnologia EMV, EMV Contactless sau Digital Wallet** – pe un Dispozitiv activ cu cip care are o aprobare/certificare valabilă și actuală EMVCo (www.emvco.com) și este capabil să proceseze Tranzacții cu Carduri Cip conforme cu AEIPS. (Comercianții din S.U.A. trebuie să includă tehnologia Contactless)
- **Criptare Integrală (P2PE)** – comunicată Împuternicitului Comerciantului folosind un sistem autorizat de PCI SSC sau un sistem de Criptare Integrală autorizat de QSA
- **Tokenizare** – soluția de tokenizare implementată trebuie:
  - să respecte specificațiile EMVCo,
  - să fie securizată, procesată, stocată, transmisă și integral gestionată de un furnizor de servicii terț cu conformitate PCI și
  - Tokenul nu poate inversat pentru a dezvălui Numere de Cont Primar (PAN) Comerciantului.

Comercianții eligibili pentru Programul de Îmbunătățire a Tehnologiei cu privire la Securitate au redus cerințele Documentației de Validare PCI, potrivit descrierii din Acțiune 3: „Completarea Documentației de Validare pe care Dvs. trebuie să o trimiteți către American Express" de mai jos.

Acțiune 3: Completarea Documentației de Validare pe care Dvs. trebuie să o trimiteți către American Express

Următoarele documente sunt necesare în funcție de diferitele niveluri ale Comercianților și ale Furnizorilor de Servicii, astfel cum sunt acestea prezentate în Tabelul A-2: Documentația de Validare a Comercianților și Tabelul A-3: Documentația de Validare a Furnizorilor de Servicii de mai sus.

Trebuie să furnizați Atestarea Conformității (AOC) pentru tipul de evaluare aplicabil. AOC este o declarație a statutului conformității dvs. și, ca atare, trebuie să fie semnat și datat la nivelul adecvat din conducerea organizației dvs.

Pe lângă AOC, American Express vă poate solicita să furnizați un exemplar din întreaga evaluare și, la propria noastră discreție, documente justificative suplimentare care să demonstreze respectarea cerințelor PCI DSS. Această Documentație de Validare se completează pe cheltuiala dvs.

Raport privind Conformitatea și Atestarea Conformității (ROC AOC) - (Cerință Anuală) – Raportul privind Conformitatea consemnează rezultatele unei examinări detaliate la fața locului a echipamentelor, sistemelor și rețelelor dvs. (și a componentelor acestora), unde se stochează, procesează sau transmit Datele Titularului Cardului sau Date Sensibile de Autentificare (sau ambele). Există două versiuni: una pentru Comercianți și alta pentru Furnizorii de Servicii. Raportul privind Conformitatea trebuie efectuat de:

- un QSA; sau
- un Expert Intern de Securitate (ISA), cu atestarea de către directorul dvs. executiv, directorul dvs. financiar, coordonatorul pentru securitatea informației sau de director în general

ROC AOC trebuie să fie semnat și datat de un QSA sau ISA și nivelul autorizat de conducere din cadrul organizației dvs. și să fie pus la dispoziția American Express cel puțin o dată pe an.

Chestionarul de Autoevaluare și Atestarea Conformității (SAQ AOC) - (Cerință Anuală) – Chestionarul de Autoevaluare permite autoexaminarea detaliată a echipamentelor, sistemelor și rețelelor dvs. (și a componentelor acestora), unde se stochează, procesează sau transmit Datele Titularului Cardului sau Date Sensibile de Autentificare (sau ambele). SAQ are mai multe versiuni. Veți selecta una sau mai multe, în funcție de Mediul de Date al Titularului de Card.

SAQ poate fi completat de personal din cadrul Companiei dvs. care este calificat să ofere răspunsuri precise și exhaustive la întrebări sau puteți angaja un QSA care să vă asiste. SAQ AOC trebuie să fie semnat și datat de nivelul autorizat de conducere din cadrul organizației dvs. și să fie pus la dispoziția American Express cel puțin o dată pe an.

Rezumat de Scanare a Vulnerabilităților Rețelei Externe cu Furnizor Autorizat de Scanare (Scanare ASV) - (Cerință la 90 de Zile) – O scanare externă a vulnerabilităților este un test de la distanță care identifică potențiale puncte slabe, vulnerabilități și configurații eronate ale componentelor care utilizează internet din Mediul dvs. de Date al Titularului de Card (de ex. site-uri, aplicații, servere web, servere de e-mail, domenii care utilizează internetul sau gazde).

Scanarea ASV trebuie efectuată de către un Furnizor Autorizat de Scanare (ASV).

Dacă SAQ impune acest lucru, trebuie să se completeze și să se trimită către American Express cel puțin la fiecare 90 de zile Raportul de Scanare ASV pentru Atestarea Conformității Scanării (AOSC) sau rezumatul executiv al scanării, inclusiv numărul de ținte scanate, certificarea respectării procedurilor de scanare PCI DSS de către rezultate și starea de conformitate completată prin ASV.

Dacă se trimite un ROC AOC sau STEP, nu este necesar să furnizați un rezumat executiv pentru AOSC sau Scanarea ASV, cu excepția solicitărilor specifice. Pentru evitarea neclarităților, Scanările sunt obligatorii dacă acest lucru este solicitat de SAQ aplicabil.

Documentația de Validare a Atestării STEP (STEP) - (Cerință Anuală) – STEP este disponibil doar pentru Comercianții care satisfac criteriile indicate în Acțiune 2: „Înțelegerea Nivelului Dvs. de Comerciant/Furnizor de Servicii și a Cerințelor Dvs. de Documentație de Validare” de mai sus. În cazul în care compania dvs. îndeplinește condițiile, trebuie să completați și să trimiteți anual formularul pentru Atestarea STEP către American Express. Formularul pentru Atestarea STEP Anuală este disponibil pentru descărcarea din Portal. Vă puteți și contacta Managerul de Clienți sau trimite o solicitare scrisă către American Express la AXPPCIComplianceProgram@aexp.com.

Neconformitatea cu PCI DSS - (Cerință Anuală, la 90 de Zile și/sau Ad-hoc) – Dacă nu respectați PCI DSS, trebuie să trimiteți un Rezumat cu Instrumentele de Abordare Prioritizate PCI (PAT) (se poate descărca de pe site-ul PCI Security Standards Council).

Rezumatul PAT trebuie să desemneze o dată de remediere, care să nu depășească douăsprezece (12) luni de la data completării documentului, pentru a respecta cerințele de conformitate. Dvs. trebuie să furnizați către American Express actualizări periodice ale progresului în ceea ce privește remedierea Stării de Neconformitate

(Comercianții de Nivel 1, Nivel 2, Nivel 3 și Nivel 4; toți Furnizorii de Servicii). Acțiunile de remediere necesare pentru a respecta cerințele de conformitate PCI DSS se vor realiza pe cheltuiala dvs.

American Express nu va impune taxe de neconformitate înainte de data remedierii. Conform Tabelului A-4 Taxă de Neconformitate, vă mențineți toate obligațiile de despăgubire față de American Express în cazul unui Incident de Date și vă asumați răspunderea față de toate celelalte prevederi ale acestei politici.

American Express, la propria sa direcție, își menține dreptul a de impune taxe de neconformitate dacă:

- nu s-a trimis un Formular de Abordare Prioritizată PCI în conformitate cu cerințele prevăzute în această secțiune,
- etapele de remediere indicate în Formularul de Abordare Prioritizată PCI pentru Starea de Neconformitate nu au fost îndeplinite,
- oricare dintre cerințele din Formularul de Abordare Prioritizată PCI pentru Starea de Neconformitate nu au fost îndeplinite sau
- documentația de conformitate obligatorie nu a fost furnizată către American Express până la un termen aplicabil sau la cerere.

Comercianților/Furnizorilor de Servicii care nu respectă cerințele detaliate în Acțiune 2: Înțelegerea Nivelului Dvs. de Comerciant/Furnizor de Servicii și a Cerințelor Dvs. de Documentație de Validare, li se pot percepe taxele indicate în Acțiune 4: Trimiterea Documentației de Validare către American Express.

Pentru evitarea neclarităților, Comercianții care nu respectă PCI DSS nu sunt eligibili pentru STEP.

Acțiune 4: Trimiterea Documentației de Validare către American Express

Toți Comercianții și Furnizorii de Servicii care trebuie să participe la Program trebuie să trimită Documentația de Validare marcată cu „obligatoriu" în tabelele de la Acțiune 2: „Înțelegerea Nivelului Dvs. de Comerciant/Furnizor de Servicii și a Cerințelor Dvs. de Documentație de Validare" către American Express până la termenele aplicabile.

Trebuie să trimiteți Documentația dvs. de Validare către American Express prin Portalul furnizat de Administratorul de Program selectat de American Express. Prin trimiterea Documentației de Validare, declarați și garantați către American Express că următoarele afirmații sunt adevărate (în măsura posibilităților dvs.):

- Evaluarea a fost completă și exhaustivă;
- Starea PCI DSS este reprezentantă cu exactitate la momentul finalizării, indiferent dacă s-a trimis Atestarea Conformității (AOC) sau un Rezumat cu Instrumentele de Abordare Prioritizate PCI (PAT) pentru neconformitate;
- Aveți autorizația de a divulga informațiile cuprinse aici și furnizați Documentația de Validare către American Express fără a încălca drepturile altor părți.

Taxele de Neconformitate și Rezilierea Acordului

American Express are dreptul de a vă impune taxe de neconformitate și de a rezilia Acordul dacă nu îndepliniți aceste cerințe sau nu furnizați documentația de validare obligatorie către American Express până la termenul aplicabil. American Express va încerca să înștiințeze persoana de contact pentru securitatea datelor privind termenul aplicabil pentru fiecare perioadă de raportare anuală și trimestrială.

Tabelul A-4: Taxă de Neconformitate

Descriere*	Comerciant de Nivel 1 sau Furnizor de Servicii de Nivel 1	Comerciant de Nivel 2 sau Furnizor de Servicii de Nivel 2	Comerciant de Nivel 3 sau Nivel 4
Se va evalua aplicarea unei taxe de neconformitate dacă documentația de validare nu este primită până la expirarea primului termen.	25.000 USD	5.000 USD	50 USD
Se va evalua aplicarea unei taxe de neconformitate suplimentare dacă documentația de validare nu este primită până la expirarea celui de-al doilea termen.	35.000 USD	10.000 USD	100 USD
Se va evalua aplicarea unei taxe de neconformitate suplimentare dacă documentația de validare nu este primită până la expirarea celui de-al treilea termen. **NOTĂ:** Taxele de neconformitate se vor aplica în continuare până la trimiterea documentației de validare.	45.000 USD	15.000 USD	250 USD

* Taxele de neconformitate vor fi evaluate în echivalențe în Moneda Locală.

* Nu se aplică în Argentina.

Dacă obligațiile dvs. privind documentația de conformitate PCI DSS nu sunt îndeplinite, atunci American Express are dreptul să impună taxele de neconformitate cumulativ, să rețină plăți și/sau să rezilieze Acordul.

Secțiunea 3 Obligații de Gestionare a Incidentelor de Date

Dvs. trebuie să informați imediat American Express și în niciun caz mai târziu de șaptezeci și două (72) de ore de la descoperirea unui Incident de Date.

Pentru a înștiința American Express, contactați Programul de răspuns la incidente Enterprise American Express (*EIRP*) gratis la 1.888.732.3750 sau la 1.602.537.3021, sau prin e-mail la EIRP@aexp.com. Dvs. trebuie să desemnați o persoană fizică de contact pentru Incidentele de Date. În plus:

- Trebuie să desfășurați o investigație aprofundată asupra fiecărui Incident de Date și să transmiteți imediat către American Express toate Numerele de Card Compromise. American Express își rezervă dreptul de a desfășura propria analiză internă pentru a identifica datele incluse în Incidentul de Date.

În cazul Incidentelor de Date cu mai puțin de 10.000 de Numere de Carduri unice, trebuie să se transmită către American Express un rezumat al investigației în decurs de zece (10) zile lucrătoare de la finalizarea lui.

- Rezumatele investigațiilor trebuie să conțină următoarele informații: rezumatul incidentului, descrierea mediului(iilor) afectat(e), cronologia evenimentelor, datele calendaristice importante, detalii privind impactul și gradul de expunere a datelor, acțiunile de izolare și remediere și o atestare a lipsei indiciilor că și alte date American Express sunt expuse riscurilor.

În cazul Incidentelor de Date care implică cel puțin 10.000 de Numere de Card, Dvs. trebuie să angajați un PCI PFI pentru a efectua această investigație în termen de cinci (5) zile de la descoperirea unui Incident de Date.

- Raportul necenzurat al investigației de fraudă trebuie transmis către American Express în termen de zece (10) zile lucrătoare de la finalizare.
- Rapoartele de investigație privind frauda trebuie să fie întocmite utilizând Modelul actual de Raport Final privind Incidentele de Fraudă disponibil la PCI. Astfel de rapoarte trebuie să includă comentarii privind frauda, rapoarte privind conformitatea și toate celelalte informații referitoare la Incidentul de Date; trebuie să identifice cauza Incidentului de Date; trebuie să confirme dacă Dvs. ați respectat sau nu standardul PCI DSS la momentul Incidentului de Date; și să verifice capacitatea acestuia de a preveni viitoarele Incidente de Date prin (i) furnizarea unui plan pentru remedierea tuturor deficiențelor PCI DSS și (ii) participarea la programul de conformitate American Express (după cum este descris mai jos). La cererea American Express, dvs. veți furniza validarea obținută de la un Evaluator de Securitate Calificat (QSA) potrivit căreia deficiențele au fost remediate.

Fără a aduce atingere paragrafelor de mai sus din prezenta Secțiune 3, „Obligații de Gestionare a Incidentelor de Date":

- American Express poate, la propria sa discreție, să vă solicite să angajați un PFI pentru a desfășura o investigație asupra unui Incident de Date pentru Incidente de Date care implică mai puțin de 10.000 de Numere de Carduri unice sau în situații în care mai multe incidente s-au petrecut într-o perioadă de 12 luni. Orice astfel de investigație trebuie să respecte cerințele stabilite mai sus în această Secțiune 3, „Obligații de Gestionare a Incidentelor de Date" și trebuie finalizată în intervalul de timp cerut de American Express.
- American Express poate, la discreția sa, să angajeze separat un PFI pentru a efectua o investigație pentru orice Incident de Date și vă poate percepe costul unei astfel de investigații.

Trebuie să evaluați Incidentul de Date conform legilor globale aplicabile de notificare a încălcării securității datelor și, când se consideră necesar, să notificați autoritățile de reglementare aplicabile și Titularii de Card afectați în conformitate cu respectivele legi de notificare. Dacă ați stabilit că Furnizorul dvs. de Servicii sau o altă entitate poartă răspunderea pentru raportarea Incidentului de Date, trebuie să înștiințați respectivul Furnizor de Servicii sau entitate de datoria sa de a-și evalua obligațiile de raportare conform legilor de notificare privind încălcarea securității datelor. Dvs. trebuie să fiți de acord să obțineți aprobare scrisă de la American Express înainte de a face trimitere la sau a numi American Express în orice comunicate cu Titularii de Card privind Incidentul de Date. Dvs. trebuie să fiți de acord să colaborați cu American Express pentru a oferi detalii și a remedia toate problemele cauzate de Incidentul de Date, inclusiv să furnizați (și să obțineți eventuale permisiuni necesare pentru a furniza) către American Express toate informațiile corespunzătoare pentru a verifica capacitatea Dvs. de a preveni viitoare Incidente de Date într-o manieră compatibilă cu Acordul.

Fără a aduce atingere niciunei eventuale obligații de confidențialitate stabilite în mod contrar de Acord, American Express are dreptul de a divulga informații despre orice Incident de Date către Titularii Cardurilor American Express, emitenți, alți participanți la Rețeaua American Express și publicul larg, conform prevederilor legale aplicabile; prin hotărâre judecătorească, administrativă sau de reglementare, prin decret, citație, solicitare sau alt proces pentru a reduce riscul de fraudă sau alte daune, sau altfel în măsura în care acest lucru este adecvat pentru funcționarea Rețelei American Express.

Cum trebuie să procedați dacă ați avut un Incident de Date?

Parcurgeți aceste etape dacă ați identificat un Incident de Date în compania dvs.

Etapa 1:

Completați Formularul de Înștiințare Inițială privind Incidentele de Date la Comercianți și trimiteți-l prin e-mail la EIRP@aexp.com în decurs de 72 de ore de la descoperirea Incidentului de Date.

Etapa 2:

Efectuați o investigație detaliată; s-ar putea să trebuiască să angajați un Investigator de Fraudă pentru Payment Card Industry (PCI).

Etapa 3:

Puneți-ne fără întârziere la dispoziție toate numerele de Carduri American Express® compromise.

Etapa 4:

Colaborați alături de noi pentru a ne ajuta să remediem orice probleme care decurg din Incidentul de Date.

Consultați Secțiunea 3, „Obligații de Gestionare a Incidentelor de Date" pentru detalii suplimentare privind Obligațiile de Gestionare a Incidentelor de Date.

Aveți și alte întrebări?

SUA: (888) 732-3750 (gratuit)

Internațional: +1 (602) 537-3021

EIRP@aexp.com

Secțiunea 4 Obligații de Despăgubire în Urma Unui Incident de Date

Obligațiile Dvs. de despăgubire față de American Express în conformitate cu Acordul privind Incidentele de Date sunt stabilite, fără ca American Express să renunțe la alte drepturi și căi de atac, în conformitate cu Secțiunea 4, „Obligații de Despăgubire în Urma Unui Incident de Date". În plus față de obligațiile Dvs. de despăgubire (dacă există), dvs. puteți fi supus unei taxe de neconformitate privind Incidentul de Date, așa cum este descris mai jos în această Secțiune 4, „Obligații de Despăgubire în Urma Unui Incident de Date".

Dvs. veți compensa American Express la o rată de 5 USD per număr de cont, pentru Incidente de Date care implică:

- 10.000 sau mai multe Numere de Carduri American Express cu oricare dintre următoarele:
  - Date Sensibile de Autentificare sau
  - Data Expirării

Cu toate acestea, American Express nu vă va solicita despăgubiri pentru un Incident de Date care implică:

- mai puțin de de 10.000 de Numere de Card American Express sau
- mai mult de 10.000 de Numere de Card American Express, dacă îndepliniți următoarele condiții:
  - ați notificat American Express privind Incidentul de Date conform Secțiunii 3, „Obligații de Gestionare a Incidentelor de Date",
  - la momentul Incidentului de Date, dvs. îndepliniați cerințele PCI DSS (acest lucru a fost determinat prin investigația PFI referitoare la Incidentul de Date) și
  - Incidentul de Date nu a fost cauzat de comportamentul culpabil al dvs. sau al Părților Interesate.

Fără a aduce atingere paragrafelor de mai sus din prezenta Secțiune 4, „Obligații de Despăgubire în Urma Unui Incident de Date", pentru orice Incident de Date, indiferent de numărul de Numere de Carduri American Express, veți plăti către American Express o taxă de nerespectare a Incidentului de Date care să nu depășească 100.000 USD per Incident de Date (așa cum este stabilit de American Express la discreția sa) în cazul în care dvs. nu respectați oricare dintre obligațiile prevăzute în Secțiunea 3, „Obligații de Gestionare a Incidentelor de Date". Pentru evitarea oricăror neclarități, taxa totală de neconformitate privind Incidentul de Date evaluată pentru orice Incident de Date nu va depăși 100.000 USD.

American Express va exclude din calculele sale orice Număr de Cont al Cardurilor American Express care a fost inclus într-o cerere anterioară de despăgubire pentru Incidente de Date depusă în termen de douăsprezece (12) luni înainte de Data Notificării. Toate calculele efectuate de American Express pe baza acestei metodologii sunt definitive.

American Express vă poate factura pentru întreaga sumă a obligațiilor dvs. de despăgubire pentru Incidentele de Date sau poate deduce suma din plățile American Express către dvs. (sau vă poate debita Contul Bancar în consecință) în conformitate cu Acordul.

Obligațiile Dvs. de despăgubire pentru Incidentele de Date menționate mai jos nu vor fi considerate daune incidentale, indirecte, speculative, consecvente, speciale, punitive sau exemplare în cadrul Acordului, cu condiția ca aceste obligații să nu includă daune legate de sau sub formă de pierderi de profituri sau de venituri, pierderea fondului comercial sau pierderea oportunităților de afaceri.

La propria sa discreție, American Express poate reduce obligațiile de despăgubire ale Comercianților doar pentru Incidentele de Date care îndeplinesc toate criteriile următoare:

- Tehnologiile aplicabile de Reducere a Riscurilor au fost utilizate înainte de producerea Incidentului de Date și în Fereastra Evenimentului Incident de Date,
- A fost efectuată o investigație detaliată conform programului PFI (cu excepția unor prevederi contrarii convenite în prealabil, în scris),
- În raportul de fraudă se specifică în mod clar că tehnologiile de reducere a riscurilor erau utilizate pentru procesarea, stocarea și/sau transmiterea datelor în momentul producerii Incidentului de Date, și
- Dvs. nu stocați (și nu ați stocat în Fereastra Evenimentului Incident de Date) Date Sensibile de Autentificare sau Date ale Titularilor Cardurilor care nu au fost făcute indescifrabile.

În cazul în care vi se aplică o reducere a obligațiilor de despăgubire (exclusiv taxele de neconformitate), aceasta va fi determinată după cum urmează:

Tabelul A-5: Criterii de Reducere a Obligațiilor de Despăgubire

Reducerea Obligațiilor de Despăgubire	Criterii Obligatorii
Reducere Standard: 50%	>75% din totalul Tranzacțiilor au fost procesate pe Dispozitive cu Activare prin Cip[1] SAU
	Tehnologiile de Reducere a Riscurilor sunt utilizate la >75% din locațiile Comercianților[2]
Reducere Extinsă: 75% - 100%	>75% din totalul Tranzacțiilor au fost procesate pe Dispozitive cu Activare prin Cip[1] ȘI alte Tehnologii de Reducere a Riscurilor sunt utilizate la >75% din locațiile Comercianților[2]

[1] După cum este determinat în urma analizei interne American Express

[2] După cum este determinat în urma investigației PFI

- Reducerea extinsă (75% - 100%) va fi determinată pe baza procentajului mai mic de Tranzacții procesate utilizând Dispozitive cu Activare prin Cip și locații ale Comercianților care utilizează alte Tehnologii de Reducere a Riscurilor. Exemplele din Tabelul A-6: Reducerea Extinsă a Obligației de Despăgubire ilustrează calculul reducerii despăgubirii.
- Pentru a fi considerată o Tehnologie de Reducere a Riscurilor, dvs. trebuie să demonstrați utilizarea eficientă a tehnologiei conform scopului în care a fost proiectată.
- Procentajul locațiilor care utilizează Tehnologii de Reducere a Riscurilor va fi stabilit în urma investigației PFI.
- Reducerea obligației de despăgubire nu se aplică taxelor de neconformitate pentru Incidentul de Date.

Tabelul A-6: Reducerea Extinsă a Obligației de Despăgubire

Ex.	Tehnologii de Reducere a Riscurilor utilizate	Eligibil	Reducere
1	• 80% din Tranzacții pe Dispozitive cu Activare prin Cip • 0% dintre locații utilizează alte Tehnologii de Reducere a Riscurilor	Nu	50%: Reducere Standard (Reducerea Extinsă nu se aplică pentru un procentaj mai mic de 75% de utilizare a Tehnologiei de Reducere a Riscurilor)[1]
2	• 80% din Tranzacții pe Dispozitive cu Activare prin Cip • 77% dintre locații utilizează alte Tehnologii de Reducere a Riscurilor	Da	77%: Reducere extinsă (procentaj de 77% de utilizare a Tehnologiei de Reducere a Riscurilor)
3	• 93% din Tranzacții pe Dispozitive cu Activare prin Cip • 100% dintre locații utilizează alte Tehnologii de Reducere a Riscurilor	Da	93%: Reducere extinsă (93% din Tranzacții pe Dispozitive cu Activare prin Cip)
4	• 40% din Tranzacții pe Dispozitive cu Activare prin Cip • 90% dintre locații utilizează alte Tehnologii de Reducere a Riscurilor	Nu	50%: Reducere Standard (Reducerea Extinsă nu se aplică pentru un procentaj mai mic de 75% de Tranzacții pe Dispozitive cu Activare prin Cip)

[1] Un Incident de Date care implică 10.000 Conturi de Carduri American Express, la o rată de 5.00 USD pe număr de cont (10.000 x 5 USD = 50.000 USD) poate fi eligibil pentru o reducere de 50%, Obligațiile de Despăgubire fiind reduse de la 50.000 USD la 25.000 USD, excluzând eventualele taxe de neconformitate.

Secțiunea 5 Programul de Analiză Vizată (TAP)

Compromiterea datelor Titularului Cardului poate fi cauzată de lacune în securitatea datelor din Mediul de Date al Titularului de Card (CDE).

Exemple de compromitere a Datelor Titularului Cardului includ, dar nu se limitează la:

- **Punct comun de achiziție (CPP):** Titularii Cardurilor American Express raportează Tranzacții frauduloase în conturile lor de Card și sunt identificate și stabilite ca provenind din efectuarea de achiziții în Unitățile dvs.
- **Datele cardului sunt găsite:** Datele Cardului American Express și Titularului Cardului găsite online sunt legate de Tranzacțiile din Unitățile dvs.
- **Malware suspectat:** American Express suspectează că utilizați software infectat cu sau vulnerabil la cod rău intenționat.

TAP este conceput pentru a identifica potențialele compromisuri ale datelor Titularului de Card.

Atât dvs., cât și Părțile Interesate, trebuie să respectați următoarele cerințe la notificarea primită de la American Express, cu privire la un potențial compromis de date ale Titularului de Card.

- Trebuie să examinați cu promptitudine CDE pentru lacunele de securitate a datelor și să remediați orice constatări.
  - Trebuie să determinați vânzătorii terți să efectueze o investigație aprofundată a CDE în caz de externalizare.
- Trebuie să furnizați un rezumat al acțiunilor întreprinse sau planificate cu privire la eforturile dvs. de revizuire, evaluare și/sau remediere după notificarea primită de la American Express.
- Trebuie să furnizați documente actualizate de validare PCI DSS Secțiunea 2, „Programul de Conformitate PCI DSS (Validarea Periodică Importantă a Sistemelor Dvs.)".
- După caz, trebuie să angajați un Investigator Criminalist PCI PFI calificat pentru a vă examina CDE dacă dvs. sau Partea dvs. Interesată:
  - Nu poate rezolva compromisul privind datele Titularului de Card într-o perioadă de timp rezonabilă, așa cum este stabilit de American Express, sau
  - Confirmă faptul că a avut loc un Incident de Date și respectă cerințele stabilite în Secțiunea 3, „Obligații de Gestionare a Incidentelor de Date".

Tabelul A-7: Taxă de Neconformitate TAP

Descriere	Comerciant de Nivel 1 sau Furnizor de Servicii de Nivel 1	Comerciant de Nivel 2 sau Furnizor de Servicii de Nivel 2	Comerciant de Nivel 3 sau Nivel 4
Taxa de neconformitate poate fi evaluată când obligațiile TAP nu sunt satisfăcute până la primul termen.	25.000 USD	5.000 USD	1.000 USD
Taxa de neconformitate poate fi evaluată când obligațiile TAP nu sunt satisfăcute până la al doilea termen.	35.000 USD	10.000 USD	2.500 USD
Taxa de neconformitate poate fi evaluată când obligațiile TAP nu sunt satisfăcute până la al treilea termen. **NOTĂ:** *Taxele de neconformitate pot fi aplicate în continuare până când sunt îndeplinite obligațiile sau se rezolvă TAP .*	45.000 USD	15.000 USD	5.000 USD

Dacă obligațiile dvs. TAP nu sunt îndeplinite, atunci American Express are dreptul să impună taxele de neconformitate cumulativ, să rețină plăți și/sau să rezilieze Acordul.

Secțiunea 6 Confidențialitate

American Express va lua măsuri rezonabile pentru a păstra (și pentru a determina agenții și subcontractanții săi, incluzând Furnizorul Portalului, să păstreze) confidențialitatea rapoartelor dvs. cu privire la conformitate, inclusiv a Documentației de Validare și pentru a nu divulga Documentația de Validare niciunui terț (cu excepția afiliaților American Express, agenților, reprezentanților, Furnizorilor de Servicii și subcontractanților) pentru o perioadă de trei ani de la data primirii acestora, însă această obligație de confidențialitate nu se aplică Documentației de Validare care:

a. este deja cunoscută de American Express înainte de divulgare;

b. este sau devine disponibilă publicului, fără încălcarea acestui paragraf de către American Express;

c. este primită în mod legal de la un terț al American Express fără nicio obligație de confidențialitate;

d. este dezvoltată independent de American Express; sau

e. trebuie dezvăluită printr-o decizie a unei instanțe, a unei agenții administrative sau a unei autorități guvernamentale sau prin orice lege, normă sau regulament sau prin citație, solicitare de informații sau citație sau alt proces administrativ sau juridic sau prin orice anchetă formală sau informală sau investigație desfășurată de agenții sau autorități guvernamentale (incluzând orice autoritate de reglementare, inspector, examinator sau agenție de aplicare a legii).

Secțiunea 7 Declinarea Responsabilității

AMERICAN EXPRESS NEAGĂ ORICE REPREZENTĂRI, GARANȚII ȘI RĂSPUNDERI CU PRIVIRE LA POLITICA OPERAȚIONALĂ CU PRIVIRE LA SECURITATEA DATELOR, PCI DSS, A SPECIFICAȚIILOR EMV ȘI A DESEMNĂRII ȘI FUNCȚIONĂRII QSA, ASV SAU PFI (SAU A ORICĂRORA DINTRE ACESTEA), FIE EXPLICITE, IMPLICITE, STATUTARE SAU ÎN ALT MOD, INCLUZÂND ORICE GARANȚIE DE COMERCIALIZARE SAU DE BUNĂ FUNCȚIONARE PENTRU UN ANUMIT SCOP. EMITENȚII CARDURILOR AMERICAN EXPRESS NU SUNT TERȚI BENEFICIARI ÎN TEMEIUL ACESTEI POLITICI.

Secțiunea 8 Glosar

Doar pentru scopul acestei *Politici Operaționale cu privire la Securitatea Datelor*, se aplică următoarele definiții și prevalează:

Acord înseamnă Prevederile Generale, Reglementările Comercianților și eventualele programe și anexe, la modul colectiv (uneori denumite Acordul de Acceptare a Cardului în materialele noastre).

Aplicația de Plată are semnificația atribuită în Glosarul Termenilor pentru Secure Software Standard și Secure Software Life Cycle Standard, valabil la momentul respectiv și disponibil la www.pcisecuritystandards.org.

Aprobat de PCI înseamnă un Dispozitiv de Introducere a PIN-ului sau o Aplicație de Plată (sau ambele) care apare, la momentul utilizării sale, pe lista companiilor și furnizorilor autorizați care este ținută de PCI Security Standards Council, LLC, disponibilă la www.pcisecuritystandards.org.

Atestarea Conformității (AOC) înseamnă o declarație privind starea conformității dvs. cu cerințele PCI DSS, în forma furnizată de către Payment Card Industry Security Standards Council, LLC.

Atestarea Conformității Scanării (AOSC) înseamnă o declarație privind starea conformității dvs. cu PCI DSS pe baza unei scanări de rețea, în forma furnizată de către Payment Card Industry Security Standards Council, LLC.

Card cu Cip înseamnă un Card care conține un Cip și ar putea solicita un PIN ca mijloc de verificare a identității Titularului Cardului sau a informațiilor contului conținute în Cip sau ambele (denumit uneori, în materialele American Express, „smart card", „card EMV" sau un card „ICC" sau „card cu circuit integrat").

Cardul American Express sau **Card** înseamnă orice card, dispozitiv de acces la cont sau dispozitiv de plată sau serviciu care poartă numele, sigla, marca comercială, marca de serviciu, denumirea comercială a companiei American Express sau a unui afiliat al acesteia sau alte desene sau modele de proprietate furnizate de un emitent sau un număr de cont de card.

Cerințe de Securitate PCI PIN înseamnă Cerințele Payment Card Industry PIN disponibile la www.pcisecuritystandards.org.

Cerințele Payment Card Industry Security Standards Council (PCI SSC) înseamnă setul de standarde și cerințe legate de securizarea și protejarea datelor cardurilor de plată, inclusiv PCI DSS și PA DSS, disponibil la www.pcisecuritystandards.org.

Cheia de criptare („Cheia de criptare American Express") înseamnă toate cheile utilizate în procesarea, generarea, încărcarea și/sau protejarea Datelor Contului. Acestea includ, însă nu se limitează la următoarele chei:

- Chei de Criptare tip Tastă: Chei Master Zone (ZMK) și Chei Pin Zone (ZPK)
- Chei Master utilizate în dispozitive criptografice sigure: Chei Master Locale (LMK)
- Chei Cod de Siguranță al Cardului (CSCK)
- Chei PIN: Chei de Derivare de Bază (BDK), Chei de criptare PIN (PEK) și ZPK

Chestionar de Autoevaluare (SAQ) înseamnă un instrument de autoevaluare creat de Payment Card Industry Security Standards Council, LLC, destinat să evalueze și să ateste conformitatea cu PCI DSS.

Cip înseamnă un microcip încorporat pe un Card care conține informații despre Titularul Cardului și despre cont.

Comerciant înseamnă Comerciantul și toți afiliații săi care acceptă Cardurile American Express în baza unui Acord încheiat cu American Express sau afiliații săi.

Comerciant Nivelul 1 înseamnă un Comerciant cu peste 2,5 milioane de Tranzacții cu Carduri American Express sau mai mult pe an; sau orice alt Comerciant pe care American Express, din alte motive, îl consideră a fi de Nivelul 1.

Comerciant Nivelul 2 înseamnă un Comerciant cu între 50.000 și mai puțin de 2,5 milioane de Tranzacții cu Carduri American Express pe an.

Comerciant Nivelul 3 înseamnă un Comerciant cu între 10.000 și mai puțin de 50.000 de Tranzacții cu Carduri American Express pe an.

Comerciant Nivelul 4 înseamnă un Comerciant cu mai puțin de 10.000 de Tranzacții cu Carduri American Express pe an.

Consumator este definit drept un titular de card care achiziționează bunuri, servicii sau ambele.

Credit înseamnă suma Debitării pe care dvs. o restituiți Titularilor Cardurilor pentru achiziții sau plăți efectuate pe Card.

Criptarea Integrală (P2PE) înseamnă o soluție care protejează criptografic datele contului din punctul în care comerciantul acceptă cardul de plată până în punctul securizat de decriptare.

Data Notificării înseamnă data stabilită de către American Express, la care emitenții primesc notificarea referitoare la Incidentul de Date. Această dată depinde de primirea de către American Express a raportului final al investigației sau a analizei interne și va fi stabilită de American Express după cum crede de cuviință.

Datele Tranzacției înseamnă toate informațiile solicitate de American Express, care evidențiază una sau mai multe Tranzacții, inclusiv informații obținute la punctul de vânzare, informații obținute sau generate în timpul Autorizării și Trimiterii și eventuale Stornări.

Datele Titularului de Card înseamnă cel puțin numărul de cont primar (PAN) complet și izolat sau PAN complet plus oricare dintre următoarele: numele titularului de card, data expirării și/sau codul de serviciu. Consultați Date Sensibile de Autentificare pentru elemente de date suplimentare care ar putea fi transmise sau procesate (însă nu și stocate) în cadrul tranzacției de plată.

Date Sensibile de Autentificare înseamnă informațiile legate de securitate utilizate la autentificarea Titularilor de Card și/sau autorizarea tranzacțiilor cu cardul de plăți. Aceste informații includ, însă nu sunt limitate la, coduri de verificare a cardului, informații complete de bandă (de pe banda magnetică sau echivalentul de pe cip), PIN-uri și blocuri cu PIN.

Datele de Cont constau din Datele Titularului de Card și/sau date sensibile de autentificare. Consultați Datele Titularului de Card și Datele Sensibile de Autentificare.

Debitare înseamnă o plată sau o achiziție făcută pe Card.

Dispozitiv cu Activare prin Cip înseamnă un dispozitiv al unui punct de vânzare care dispune de o aprobare/certificare valabilă EMVCo (www.emvco.com) și care este capabil să proceseze Tranzacții cu Carduri Cip care sunt conforme cu AEIPS.

Dispozitiv pentru Introducere PIN are sensul atribuit acestuia prin Glosarul de Termeni pentru Payment Card Industry PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, disponibil la www.pcisecuritystandards.org.

Documentația de Validare înseamnă AOC furnizat în legătură cu Evaluarea Anuală a Securității la Fața Locului sau SAQ, AOSC și rezumatele concluziilor Scanărilor Trimestriale ale Rețelei sau Atestatul Anual al Programului de Îmbunătățire a Tehnologiei cu privire la Securitate.

Emitent înseamnă orice Entitate (inclusiv American Express și Afiliații săi) licențiată de American Express sau de un Afiliat American Express pentru a emite Carduri și pentru a se angaja în activitatea de emitere a Cardurilor.

Expert Autorizat de Securitate (QSA) înseamnă o entitate care a fost autorizată de către Payment Card Industry Security Standards Council, LLC pentru a valida respectarea cerințelor PCI DSS.

Fereastra Evenimentului Incident de Date înseamnă intervalul de intruziune (sau o perioadă de timp similar determinată) stabilit în raportul de investigație final (de ex. raportul PFI) sau, dacă nu se cunoaște, cu până la 365 de zile înainte de ultima Dată a Notificării aferente Numerelor de Card potențial Compromise și implicate într-o Compromitere a Datelor raportată către noi.

Francizat înseamnă terț deținut și operat în mod independent (inclusiv un francizat, licențiat sau filială) altul decât un Afiliat, care este autorizat de un Francizor să opereze o franciză și care a încheiat un acord scris cu Francizorul prin care afișează în mod consecvent elemente de identificare exterioare care îl asociază în mod evident cu Mărcile Francizorului sau se prezintă publicului ca un membru al grupului de companii al Francizorului.

Francizor înseamnă operatorul unei afaceri care autorizează persoane sau Entități (Francizați) să distribuie bunuri și/sau servicii sub marca sau să opereze folosind marca operatorului; acordă asistență Francizaților în desfășurarea activității acestora sau influențează modul de funcționare al Francizaților; și necesită plata unei taxe de către Francizați.

Furnizor Autorizat de Scanare (ASV) înseamnă o Entitate care a fost autorizată de Payment Card Industry Security Standards Council, LLC pentru a valida respectarea anumitor cerințe PCI DSS prin efectuarea de scanări de vulnerabilitate a mediilor care utilizează internetul.

Furnizor de Servicii Nivelul 1 înseamnă un Furnizor de Servicii cu peste 2,5 milioane de Tranzacții cu Carduri American Express sau mai mult pe an; sau orice alt Furnizor de Servicii pe care American Express, din alte motive, îl consideră a fi de Nivelul 1.

Furnizor de Servicii Nivelul 2 înseamnă un Furnizor de Servicii cu mai puțin de 2,5 milioane de Tranzacții cu Carduri American Express pe an; sau orice alt Furnizor de servicii pe care American Express nu îl consideră a fi de Nivelul 1.

Furnizori de Servicii înseamnă împuterniciți autorizați, terți împuterniciți, furnizorii de gateway-uri, integratorii de sisteme POS și orice alți furnizori de Sisteme POS ai Comercianților sau alte soluții sau servicii de procesare a plăților.

Incident de Date înseamnă un incident care implică compromiterea sau suspiciunea de compromitere a cheilor de criptare American Express sau cel puțin un număr de cont al Cardului American Express în care există:

- un acces neautorizat sau folosirea Cheilor de Criptare, a Datelor Titularilor Cardurilor sau a Datelor Sensibile de Autentificare (sau o combinație a fiecăreia dintre acestea) care sunt stocate, procesate sau transmise pe echipamentul Comerciantului, prin sistemele și/sau rețelele (sau componentele acestora) ale Comerciantului sau a căror utilizare o mandatează, furnizează sau pun la dispoziție;
- o utilizare a acestor Chei de Criptare, a Datelor Titularilor Cardurilor sau a Datelor Sensibile de Autentificare (sau a unei combinații a fiecăreia dintre acestea), în alt mod decât în conformitate cu Acordul; și/sau
- suspiciunea sau confirmarea unei pierderi, furt sau deturnare prin orice mijloace a oricăror fișiere media, materiale, înregistrări sau informații care conțin astfel de Chei de Criptare, Date ale Titularilor Cardurilor sau Date Sensibile de Autentificare (o combinație a fiecăreia dintre acestea).

Informații despre Titularul Cardului înseamnă informații despre Titularii Cardurilor și Tranzacțiile cu Carduri American Express, inclusiv numele, adresele, numerele de cont ale cardului și numerele de identificare ale cardurilor (CID).

Înregistrare de Credit înseamnă o înregistrare de Credit care ne respectă cerințele.

Înregistrare privind Debitarea înseamnă o înregistrare reproductibilă (atât tipărită, cât și electronică) a unei Debitări, care respectă cerințele noastre și conține Numărul de Card, data Tranzacției, suma în dolari, Aprobarea, semnătura Titularului de Card (dacă este cazul) și alte informații.

Investigator de Fraudă PCI (PFI) înseamnă o entitate autorizată de către Payment Card Industry Security Standards Council, LLC să efectueze investigații de fraudă cu privire la încălcarea sau compromiterea Datelor de pe un Card de plăți.

Împuternicit înseamnă un furnizor de servicii al Comercianților care facilitează autorizarea și procesarea trimiterilor către rețeaua American Express.

Mediul de Date al Titularului de Card (CDE) înseamnă persoanele, procesele și tehnologia care stochează, procesează sau transmit date referitoare la titularul de card sau date sensibile de autentificare.

Modelul de Raport Final privind Incidentele de Fraudă înseamnă modelul pus la dispoziție de PCI Security Standards Council, disponibil la adresa www.pcisecuritystandards.org.

Nivelul de Comerciant înseamnă denumirea pe care o alocăm Comercianților în raport cu obligațiile lor de validare a conformității PCI DSS, conform descrierii din Secțiunea 2, „Programul de Conformitate PCI DSS (Validarea Periodică Importantă a Sistemelor Dvs.)".

Număr Card înseamnă numărul unic de identificare pe care Emitentul îl atribuie Cardului atunci când este emis.

Număr de Card Compromis înseamnă un număr de cont al Cardului American Express legat de un Incident de Date.

Numărul de Cont Primar (PAN) are semnificația care i-a fost atribuită în Glosarul Terminologic pentru PCI DSS valabil la momentul respectiv.

Payment Card Industry Data Security Standard (PCI DSS) înseamnă Standardul de Securitate a Datelor din Industria Cardurilor de Plată, care este disponibil la www.pcisecuritystandards.org.

Părți Interesate înseamnă oricare sau toți angajații, agenții, reprezentanții, subcontractanții, Procesatorii, Furnizorii de Servicii, furnizorii de echipamente sau sisteme sau soluții de procesare a plăților de tip punct de vânzare (POS), Entități asociate cu contul dvs. de Comerciant American Express și orice altă parte căreia i-ați putea furniza acces la Datele Titularului de Card sau Datele de Autentificare Sensibile (sau ambele) în conformitate cu Acordul.

PCI DSS: Payment Card Industry Data Security Standard, disponibil la www.pcisecuritystandards.org.

Portalul înseamnă sistemul de raportare furnizat de Administratorul Programului PCI American Express selectat de American Express. Comercianții și Furnizorii de Servicii au obligația de a folosi Portalul pentru a trimite documentația de validare PCI către American Express.

Programul înseamnă Programul de Conformitate PCI al American Express.

Programul de Analiză Vizată înseamnă un program care oferă identificarea timpurie a unui potențial compromis de date ale Titularului de Card din Mediul de Date al Titularului de Card (CDE) ce vă aparține. Consultați Secțiunea 5, „Programul de Analiză Vizată (TAP)".

Programul de Îmbunătățire a Tehnologiilor cu privire la Securitate (STEP) înseamnă programul American Express prin care Comercianții sunt încurajați să implementeze tehnologii care îmbunătățesc securitatea datelor.

Sistem de la Punct de Vânzare (POS) înseamnă un sistem sau un echipament de procesare a informațiilor, inclusiv un terminal, un computer personal, un registru electronic de numerar, un cititor contactless, un mecanism sau un proces de plată utilizat de un Comerciant, pentru a obține autorizații sau pentru a culege date despre Tranzacții, sau pentru amândouă.

Soluție Autorizată pentru Criptarea Integrală (P2PE), inclusă pe lista de soluții validate PCI SSC sau validată de către un Expert Autorizat de Securitate pentru PCI SSC al unei Companii tip P2PE.

Specificații EMV înseamnă specificațiile emise de EMVCo, LLC, disponibile la http://www.emvco.com.

Tehnologie de Reducere a Riscurilor înseamnă soluții tehnologice care îmbunătățesc securitatea Datelor Titularului Cardului sau Datelor Sensibile de Autentificare American Express, după cum este determinat de American Express. Pentru a fi considerată o Tehnologie de Reducere a Riscurilor, dvs. trebuie să demonstrați

utilizarea eficientă a tehnologiei conform scopului în care a fost proiectată. Exemplele le includ pe următoarele, însă nu numai: EMV, Criptare Integrală și tokenizare.

Titularul Cardului înseamnă o persoană fizică sau o entitate (i) care a încheiat un acord de constituire a unui cont de Card cu un emitent sau (ii) al cărei nume apare pe Card.

Titular de Card înseamnă un client căruia i s-a emis un card de plăți sau orice persoană autorizată să folosească cardul de plăți.

Token înseamnă tokenul criptografic care înlocuiește PAN, fiind bazat pe un indice dat pentru o valoare nepreconizabilă.

Tranzacție înseamnă o Debitare, un Credit, un Avans în Cash (sau alt acces la cash) sau Tranzacție ATM realizate prin intermediul unui Card.

Tranzacție EMV înseamnă o Tranzacție cu un card cu circuit integrat (denumit uneori „Card IC" „card cu cip" „smart card," „EMV card," sau „ICC") efectuată pe un terminal al unui punct de vânzare (POS) compatibil cu carduri IC cu o aprobare curentă și valabilă de tip EMV. Tipurile de aprobări EMV sunt disponibile la http://www.emvco.com.

Tranzacțiile tip Plăți în scop de business (BIP) înseamnă o soluție de plăți digitală care le permite cumpărătorilor să programeze rapid și eficient plăți către furnizori (asociați cardurilor corporative).

Secțiunea 9 Site-uri Web Utile

Securitatea Datelor American Express: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

EMVCo: www.emvco.com