IBM Security Trusteer Fraud Protection

Termenii de Utilizare ("TdU") sunt alcătuiţi din aceşti Termeni de Utilizare IBM – Termeni Specifici Ofertei SaaS ("Termenii Specifici Ofertei SaaS") şi un document intitulat Termenii de Utilizare IBM – Termeni Generali ("Termenii Generali"), disponibil la următorul URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

În eventualitatea unui conflict, Termenii Specifici Ofertei SaaS vor prevala faţă de Termenii Generali. Prin comandarea, accesarea sau utilizarea IBM SaaS, Clientul este de acord cu aceşti Termeni de Utilizare.

Termenii de Utilizare sunt guvernaţi de IBM International Passport Advantage Agreement, IBM International Passport Advantage Express Agreement sau IBM International Agreement for Selected IBM SaaS Offerings, după caz ("Contractul"), care împreună cu Termenii de Utilizare reprezintă acordul complet.

1. IBM SaaS

Aceşti Termeni Specifici Ofertei SaaS acoperă următoarele oferte IBM SaaS:

1.1 Ofertele IBM SaaS Rapport

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Ofertele IBM SaaS Pinpoint

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Ofertele IBM SaaS Mobile

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

2. Indicii de Măsurare pentru Tarifare

IBM SaaS este vândut în baza unuia dintre următorii indici de măsurare pentru tarifare, după cum este specificat în Documentul Tranzacţional:

a. **Participant Eligibil** – este o unitate de măsură pentru obţinerea IBM SaaS. Fiecare persoană fizică sau entitate eligibilă pentru a participa la orice program de furnizare de servicii gestionat sau urmărit de IBM SaaS este un Participant Eligibil. Trebuie obţinute drepturi suficiente pentru a acoperi Participanţii Eligibili gestionaţi sau urmăriţi în IBM SaaS pe durata perioadei de măsurare specificate în Documentul Tranzacţional al Clientului.

   Fiecare program de furnizare a serviciilor gestionat de IBM SaaS este analizat separat şi apoi adăugat la celelalte. Persoanele individuale sau entităţile eligibile pentru mai multe programe de furnizare a serviciilor necesită drepturi de utilizare separate.

   Pentru aceste oferte, un program de furnizare a serviciilor include o singură Aplicaţie Business sau Retail a Clientului, cu o pagină principală de logare şi pagini conexe pentru fiecare Aplicaţie Business sau Retail. Un Participant Eligibil este un utilizator final al Clientului, care are acreditări de logare pentru Aplicaţia Business sau Retail.

b. **Dispozitiv Client** – este o unitate de măsură pentru obţinerea IBM SaaS. Un Dispozitiv Client este un dispozitiv informatic cu un singur utilizator, un senzor pentru un scop special sau un dispozitiv de telemetrie, care necesită executarea sau primirea pentru execuţie a unui set de comenzi, proceduri sau aplicaţii de la sau furnizarea datelor către alt sistem informatic, numit de obicei server, sau care este gestionat în alt fel de server. Mai multe Dispozitive Client pot partaja accesul la un server comun. Un Dispozitiv Client poate avea o anumită capabilitate de procesare sau poate fi programabil, pentru a permite utilizatorului să lucreze. Clientul trebuie să obţină drepturi pentru fiecare Dispozitiv Client care rulează, furnizează date către, utilizează servicii furnizate de sau accesează în alt fel IBM SaaS pe durata perioadei de măsurare specificate în Documentul Tranzacţional al Clientului.

3. Tarife şi Facturare

Suma de plată pentru IBM SaaS este specificată într-un Document Tranzacţional.

3.1 Tarife Lunare Parţiale

Un tarif lunar parţial, după cum este specificat în Documentul Tranzacţional, poate fi evaluat prin proratare.

4. Conformitatea şi Auditarea

Accesul la ofertele IBM Security Trusteer Fraud Protection este condiţionat de protecţia unui număr maxim de Participanţi Eligibili sau Dispozitive Client, după cum este specificat în Documentul Tranzacţional. Clientului îi revine responsabilitatea de a se asigura că numărul său de Participanţi Eligibili sau Dispozitive Client nu depăşeşte numărul maxim specificat în Documentul Tranzacţional.

Poate fi efectuat un audit pentru a se verifica respectarea numărului maxim de Participanţi Eligibili sau Dispozitive Client.

5. Opţiuni pentru Reînnoirea Perioadei de Abonare IBM SaaS

În Documentul Tranzacţional al Clientului, va fi specificat dacă IBM SaaS va fi reînnoit la sfârşitul Perioadei de Abonare, prin desemnarea uneia dintre următoarele:

5.1 Reînnoire Automată

Dacă în Documentul Tranzacţional al Clientului se specifică reînnoirea automată, Clientul poate termina Perioada de Abonare IBM SaaS care expiră, printr-o cerere scrisă, trimisă către reprezentantul de vânzări IBM sau Partenerul de Afaceri IBM, cu cel puţin nouăzeci (90) de zile înaintea datei de expirare care este specificată în Documentul Tranzacţional. Dacă IBM sau Partenerul de Afaceri IBM nu primeşte o astfel de notificare privind terminarea până la data expirării, Perioada de Abonare care expiră va fi reînnoită automat pentru un an sau pentru durata Perioadei de Abonare iniţiale, după cum este specificat în Documentul Tranzacţional.

5.2 Facturare Continuă

În cazul în care Documentul Tranzacţional specifică reînnoirea Clientului ca fiind continuă, Clientul va avea acces în continuare la IBM SaaS şi va fi facturat încontinuu pentru utilizarea IBM SaaS. Pentru a întrerupe utilizarea IBM SaaS şi a opri procesul de facturare continuă, înainte cu nouăzeci (90) de zile, Clientul va trebui să trimită către IBM sau Partenerul de Afaceri IBM o notificare scrisă prin care să solicite anularea IBM SaaS. După anularea accesului Clientului, Clientul va fi facturat pentru tarifele de acces neplătite până în luna în care a devenit efectivă anularea.

5.3 Reînnoire Solicitată

Când în Documentul Tranzacţional se specifică "terminare" pentru tipul de reînnoire al Clientului, IBM SaaS se va termina la sfârşitul Perioadei de Abonare şi Clientul nu va mai avea acces la IBM SaaS. Pentru a continua să utilizeze IBM SaaS după data terminării, Clientul va trebui să plaseze o comandă cu reprezentantul de vânzări IBM sau Partenerul de Afaceri IBM, pentru a achiziţiona o nouă Perioadă de Abonare.

6. Suport Tehnic

Clientul şi Participanţii săi Eligibili pot beneficia de Suport Tehnic pentru IBM SaaS, fiind asistaţi la utilizarea IBM SaaS.

Suportul Standard este inclus în abonamentul tuturor ofertelor. Trusteer Rapport Mandatory Service, care este un add-on pentru Trusteer Rapport, are ca cerinţă preliminară Suportul Premium pentru abonamentul Trusteer Rapport de bază.

Pentru fiecare ofertă IBM SaaS, este disponibil un abonament de Suport Premium pentru un tarif suplimentar, cu excepţia ofertelor IBM Security Trusteer Mobile SDK şi a ofertelor IBM Security Trusteer Rapport Mandatory Service.

Suport Standard:

- Suport între orele 8-17, ora locală.
- Clienţii şi Participanţii lor Eligibili pot trimite electronic tichete de suport, după cum se descrie pe larg în Software as a Service [SaaS] Support Handbook.
- Clienţii pot accesa Client Support Portal pentru notificări, documente, rapoarte de caz şi întrebări puse frecvent (FAQ), la: http://www-01.ibm.com/software/security/trusteer/support/.
- Pentru opţiunile de suport şi alte detalii, consultaţi IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

Suport Premium:

- Suport 24x7 pentru toate severităţile.
- Clienţii pot beneficia de suport direct prin telefon.
- Clienţii şi Participanţii lor Eligibili pot trimite electronic tichete de suport, după cum se descrie pe larg în Software as a Service [SaaS] Support Handbook.
- Clienţii pot accesa Client Support Portal pentru notificări, documente, rapoarte de caz şi întrebări puse frecvent (FAQ), la: http://www-01.ibm.com/software/security/trusteer/support/.

- Pentru opţiunile de suport şi alte detalii, consultaţi IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

7. Termeni Suplimentari pentru Oferta IBM SaaS

7.1 Conformitatea Safe Harbor

IBM se conformează cadrului de lucru U.S. – EU Safe Harbor Framework, elaborat de Departamentul de Comerţ al Statelor Unite în colaborare cu Comisia Europeană. Produsele IBM Security Trusteer sunt incluse în certificarea IBM pentru EU-U.S. Safe Harbor. Pentru informaţii suplimentare privind Safe Harbor şi lista de companii Safe Harbor, vizitaţi http://export.gov/safeharbor/.

7.2 Creşterea Tarifului pentru Abonamentul Anual al Clientului

IBM îşi rezervă dreptul de a ajusta tariful abonamentului pentru IBM SaaS, cel mult o dată la fiecare douăsprezece (12) luni, cu un procent care urmează să fie stabilit de IBM şi care nu depăşeşte 3%. Ajustarea tarifului pentru abonament va intra în vigoare la aniversarea datei perioadei de acoperire iniţiale. Această ajustare a tarifului nu alterează dreptul de utilizare al Clientului pentru IBM SaaS sau indicele de măsurare pentru tarifare în baza căruia este obţinut IBM SaaS. Partenerii de afaceri IBM sunt independenţi faţă de IBM şi îşi determină unilateral preţurile şi termenii.

7.3 Suport Premium

Clientul are dreptul la Suport Premium numai pentru ofertele IBM SaaS pentru care Clientul s-a abonat la oferta Suport Premium asociată.

7.4 Utilizarea Legală şi Consimţământul

Autorizarea pentru Colectarea şi Procesarea Datelor

IBM SaaS este conceput pentru a ajuta Clientul să-şi îmbunătăţească datele şi mediul de securitate. IBM SaaS va colecta informaţii de la Participanţii Eligibili şi Dispozitivele Client care interacţionează cu Aplicaţiile Business sau Retail pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS. IBM SaaS colectează informaţii care, individual sau în combinaţie, pot fi considerate Informaţii Personale în anumite jurisdicţii. Datele Personale sunt orice informaţii care pot fi utilizate pentru a identifica o anumită persoană, cum ar fi numele, adresa de e-mail, adresa de domiciliu sau numărul de telefon, şi care sunt furnizate către IBM pentru a fi stocate, procesate sau transferate în numele Clientului.

Practicile pentru colectarea şi procesarea datelor pot fi actualizate, pentru a îmbunătăţi funcţionalitatea IBM SaaS. Documentul cu descrierea completă a practicilor pentru colectarea şi procesarea datelor este actualizat ori de câte ori este necesar şi poate fi accesat de Client la cerere. Clientul autorizează IBM să colecteze aceste informaţii şi să le proceseze în conformitate cu secţiunea Transferurile Transfrontaliere şi secţiunea Confidenţialitatea Datelor, din aceşti Termeni de Utilizare, şi secţiunea Confidenţialitatea şi Securitatea Datelor, din Termenii de Utilizare – Termeni Generali.

Pentru ofertele IBM Security Trusteer Pinpoint:

Datele colectate pot include adresa IP a utilizatorului, ID-ul de utilizator criptat sau codat hash unidirecţional, cookie-uri de domeniu dacă nu sunt filtrate, vizitările Aplicaţiilor protejate şi site-urilor de phishing, locaţia geografică şi acreditările introduse pe site-urile de phishing.

Pentru ofertele IBM Security Trusteer Mobile SDK şi ofertele IBM Security Trusteer Mobile Browser:

Datele colectate pot include adresa IP a utilizatorului, ID-ul de utilizator criptat sau codat hash unidirecţional, locaţia geografică, vizitările Aplicaţiilor protejate, informaţii privind cardul SIM, numele de dispozitv şi afilierea Clientului.

Pentru ofertele IBM Security Trusteer Rapport:

Datele colectate pot include adresa IP a utilizatorului, ID-ul de utilizator criptat sau codat hash unidirecţional, evenimente de securitate, numele de utilizator şi adresa de e-mail furnizate pentru contactarea IBM în vederea obţinerii suportului pentru Client, afilierea Clientului, parola criptată introdusă pe site-urile protejate, vizitările Aplicaţiilor protejate şi a site-urilor de phishing, numărul cardului de plată criptat şi fişierele şi datele colectate de la distanţă de către personalul IBM pentru inspecţie în cazurile suspecte de malware, activitate rău intenţionată sau funcţionare necorespunzătoare.

Consimţământul avizat de la persoanele la care se referă datele:

Utilizarea acestui IBM SaaS poate implica diverse legi şi reglementări. IBM SaaS poate fi utilizat numai pentru scopuri legale şi într-o manieră legală. Clientul este de acord să utilizeze IBM SaaS în conformitate cu, şi să-şi asume întreaga responsabilitate pentru respectarea legilor, reglementărilor şi politicilor aplicabile.

Pentru ofertele IBM Security Trusteer Pinpoint şi ofertele IBM Security Trusteer Mobile SDK:

Clientul confirmă că a obţinut sau va obţine, în condiţiile unei informări complete, consimţămintele, permisiunile sau licenţele necesare pentru a permite utilizarea legală a IBM SaaS şi colectarea şi procesarea informaţiilor de către IBM prin IBM SaaS.

Pentru ofertele IBM Security Trusteer Rapport şi ofertele IBM Security Trusteer Mobile Browser:

Clientul autorizează IBM să obţină, în condiţiile unei informări complete, consimţămintele necesare pentru a permite utilizarea legală a IBM SaaS şi colectarea şi procesarea informaţiilor după cum se descrie în Acordul de Licenţă pentru Utilizatorul Final, disponibil la https://www.trusteer.com/support/end-user-license-agreement. În eventualitatea în care Clientul stabileşte că el (şi nu IBM) va gestiona comunicările cu utilizatorii pentru obţinerea consimţămintelor, Clientul confirmă că a obţinut sau va obţine, în condiţiile unei informări complete, consimţămintele, permisiunile sau licenţele necesare pentru a permite utilizarea legală a IBM SaaS şi colectarea şi procesarea informaţiilor de către IBM, ca procesor al datelor Clientului, prin IBM SaaS.

7.5 Transferurile Transfrontaliere

Clientul este de acord că IBM poate procesa Conţinutul, inclusiv orice Date Personale, în baza legilor şi cerinţelor relevante, în afara graniţelor unei ţări, la procesori şi subprocesori din următoarele ţări aflate în afara Zonei Economice Europene şi ţările considerate de Comisia Europeană ca având niveluri adecvate de securitate: S.U.A.

7.6 Confidenţialitatea Datelor

În cazul în care Clientul face disponibile Date Personale pentru IBM SaaS în Statele Membre UE, Islanda, Liechtenstein, Norvegia sau Elveţia sau în cazul în care Clientul are Participanţi Eligibili sau Dispozitive Client în aceste ţări, Clientul, ca unic controlor, desemnează IBM ca procesor în vederea procesării Datelor Personale (după cum sunt definiţi aceşti termeni în Directiva UE 95/46/EC). IBM va procesa astfel de Date Personale în măsura în care este necesar pentru a face disponibilă oferta IBM SaaS, în conformitate cu descrierile IBM publicate ale IBM SaaS, iar Clientul este de acord că orice astfel de procesare este în conformitate cu instrucţiunile Clientului. IBM va trimite în avans o notificare, cu un interval rezonabil de timp, atunci când face o modificare importantă privind locaţia de procesare sau modalitatea în care securizează Datele Personale ca parte a IBM SaaS. Clientul poate termina Perioada de Abonare curentă pentru oferta IBM SaaS afectată, prin transmiterea către IBM a unei notificări scrise într-un interval de treizeci (30) de zile de la data notificării trimise de IBM Clientului cu privire la modificarea respectivă. Clientul este de acord că IBM poate procesa Conţinutul, inclusiv orice Date Personale, în afara graniţelor unei ţări, la următorii procesori şi subprocesori:

Nume Procesor/Subprocesor	Rol (Procesor sau Subprocesor Date)	Locaţie*
Entitatea contractantă IBM	Procesor	După cum este specificat în Documentul Tranzacţional
Amazon Web Services LLC	Subprocesor	410 Terry Ave. N Seattle, WA 98109 Statele Unite
Connectria Corp.	Subprocesor	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 Statele Unite
IBM Israel Ltd.	Subprocesor	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel
IBM Corp	Subprocesor	1 New Orchard Rd. Armonk, NY 10504 Statele Unite

Clientul este de acord că IBM poate, în urma unei notificări, să modifice această listă de locaţii de ţară, atunci când determină, în mod rezonabil, că este necesar pentru provizionarea IBM SaaS.

Clientul este de acord că, pentru serviciul furnizat prin centrul de date german, după cum se determină în cursul procesului de provizionare, IBM poate procesa Conţinutul, inclusiv orice Date Personale, în afara graniţelor unei ţări, la următorii procesori şi subprocesori:

Nume Procesor/Subprocesor	Rol (Procesor sau Subprocesor Date)	Locaţie*
Entitatea contractantă IBM	Procesor	După cum este specificat în Documentul Tranzacţional
Amazon Web Services (Germania)	Subprocesor	Munchen, Germania
IBM Israel Ltd.	Subprocesor	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

Clientul este de acord că, pentru serviciul furnizat prin centrul de date japonez, după cum se determină în cursul procesului de provizionare, IBM poate procesa Conţinutul, inclusiv orice Date Personale, în afara graniţelor unei ţări, la următorii procesori şi subprocesori:

Nume Procesor/Subprocesor	Rol (Procesor sau Subprocesor Date)	Locaţie*
Entitatea contractantă IBM	Procesor	După cum este specificat în Documentul Tranzacţional
Amazon Web Services (Japonia)	Subprocesor	Tokyo, Japonia
IBM Israel Ltd.	Subprocesor	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

* Locaţiile identificate în tabelele de mai sus includ adresele birourilor corporative ale Procesorului/Subprocesorului. Centrele de date se află în ţara identificată.

Părţile, sau afiliatele lor relevante, pot încheia contracte Clauză Model UE standard separate, nemodificate, în rolurile lor corespondente, conform Deciziei CE 2010/87/EU, cu clauzele opţionale înlăturate. Toate disputele şi obligaţiile care apar în legătură cu aceste contracte, chiar dacă sunt încheiate de afiliate, vor fi tratate de către părţi ca o dispută sau obligaţie apărută între ele în baza termenilor acestui Contract.

Anexa A

1. Ofertele IBM SaaS

IBM oferă aceste servicii ca servicii şi oferte autonome sau ca servicii şi oferte adiţionale. Oferta IBM SaaS comandată este specificată în Dovada Dreptului de Utilizare (PoE) a Clientului.

1.1 Definiţiile Aplicaţiilor Business şi Retail

Produsele IBM Security Trusteer de combatere a fraudelor sunt licenţiate pentru utilizarea cu tipuri specifice de Aplicaţii. Prin definiţie, Aplicaţiile sunt de două tipuri: Retail sau Business. Sunt disponibile oferte separate pentru Aplicaţiile Retail şi Aplicaţiile Business.

- O Aplicaţie Retail este definită ca o aplicaţie bancară online, o aplicaţie mobilă sau o aplicaţie e-commerce proiectată pentru a servi consumatorii. În funcţie de politica aplicată de Client, anumite afaceri mai mici pot fi clasificate ca fiind eligibile pentru acces comercial.
- O Aplicaţie Business este definită ca o aplicaţie bancară online, o aplicaţie mobilă sau o aplicaţie e-commerce proiectată pentru a servi corporaţii, instituţii sau entităţi echivalente sau orice aplicaţie care nu este considerată Retail.

1.2 Ofertele de Abonament IBM SaaS de Bază

Ofertele Business:

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

Ofertele Retail:

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

Pentru fiecare dintre ofertele Business şi Retail, există un produs Suport Premium asociat care este disponibil în baza unui tarif suplimentar, cu excepţia ofertelor IBM Security Trusteer Mobile SDK.

1.3 Ofertele de Abonament IBM SaaS Suplimentare pentru Ofertele IBM Security Trusteer Rapport

Oferte suplimentare disponibile pentru IBM Security Trusteer Rapport for Business:

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

Oferte suplimentare disponibile pentru IBM Security Trusteer Rapport for Retail:

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

Pentru fiecare dintre add-on-urile Business şi Retail pentru ofertele IBM Security Trusteer Rapport, cu excepţia add-on-urilor IBM Security Trusteer Rapport Mandatory Service, există un produs Suport Premium asociat care este disponibil în baza unui tarif suplimentar.

Abonamentul pentru IBM Security Trusteer Rapport for Business sau IBM Security Trusteer Rapport for Retail este o cerinţă preliminară pentru ofertele de abonament IBM SaaS suplimentare asociate, listate în această secţiune.

1.4 Ofertele de Abonament IBM SaaS Suplimentare pentru Ofertele IBM Security Trusteer Pinpoint Malware Detection

Oferte suplimentare disponibile pentru IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition sau IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Oferte suplimentare disponibile pentru IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition sau IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

Abonamentul de Suport Premium este disponibil în baza unui tarif suplimentar pentru fiecare dintre ofertele IBM SaaS suplimentare, listate în această secţiune.

Abonamentul pentru ofertele IBM Security Trusteer Pinpoint Malware Detection for Business sau IBM Security Trusteer Pinpoint Malware Detection for Retail este o cerinţă preliminară pentru ofertele de abonament IBM SaaS suplimentare asociate, listate în această secţiune.

1.5 Alte Abonamente IBM SaaS Suplimentare

Orice Abonament IBM SaaS suplimentar pentru abonamentele de bază de mai sus care nu este listat aici, disponibil curent sau în stadiu de dezvoltare, nu este considerat o actualizare şi trebuie să fie acordat separat.

1.6 Definiţii

Titular de Cont – înseamnă utilizatorul final al Clientului, care a instalat software-ul pentru activarea clientului, a acceptat acordul de licenţă pentru utilizatorul final ("EULA") şi s-a autentificat cel puţin o dată în Aplicaţia Retail sau Business a Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS.

Software-ul Client al Titularului de Cont – înseamnă software-ul de activare a clientului IBM Security Trusteer Rapport, software-ul de activare a clientului IBM Security Trusteer Mobile Browser sau orice alt software de activare a clientului care este furnizat cu unele abonamente IBM SaaS pentru instalarea pe dispozitivul utilizatorului final.

Trusteer Splash – se referă la splash-ul furnizat clientului în funcţie de şabloanele de splash disponibile.

Pagina de întâmpinare – se referă la pagina găzduită de IBM care este afişată clientului cu splash-ul clientului şi pachetul descărcabil al Software-ului Client al Titularului de Cont.

2. Ofertele IBM Security Trusteer Rapport

2.1 IBM Security Trusteer Rapport for Retail şi/sau IBM Security Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport furnizează un nivel de protecţie împotriva atacurilor tip phishing şi cu malware Man-in-the-Browser (MitB). Utilizând o reţea de zeci de milioane de puncte finale de pe tot globul, IBM Security Trusteer Rapport colectează informaţii despre atacurile active phishing şi malware împotriva organizaţiilor din întreaga lume. IBM Security Trusteer Rapport aplică algoritmi comportamentali axaţi pe atacurile phishing şi previne instalarea şi operarea versiunilor de malware MitB.

Această ofertă IBM SaaS are un indice de măsurare pentru tarifare Participant Eligibil. Oferta Business este vândută în pachete de 10 Participanţi Eligibili. Oferta Retail este vândută în pachete de 100 de Participanţi Eligibili.

Această ofertă IBM SaaS include:

a. Trusteer Management Application ("TMA"):

   Aplicaţia TMA este făcută disponibilă în mediul găzduit în cloud IBM Security Trusteer şi permite Clientului (şi unui număr nelimitat de persoane care fac parte din personalul său autorizat): (i) primirea rapoartelor cu date de evenimente şi a evaluărilor de risc, (ii) vizualizarea, configurarea şi setarea politicilor privind raportarea datelor de evenimente şi (iii) vizualizarea configuraţiei software-ului de activare a clientului, licenţiat gratuit pentru public în baza acordului de licenţă pentru utilizatorul final ("EULA") şi făcut disponibil pentru descărcare pe desktop-urile şi dispozitivele (PC/MAC) Participanţilor Eligibili, numit şi suita de software Trusteer Rapport ("Software-ul Client al Titularului de Cont"). Clientul poate doar să comercializeze Software-ul Client al Titularului de Cont utilizând API-ul Rapport sau Trusteer Splash şi Clientul nu poate utiliza Software-ul Client al Titularului de Cont pentru operaţiile sale interne de afaceri sau activitatea propriilor angajaţi (alta decât utilizarea personală a angajaţilor).

b. Script Web:

   Pentru accesarea unui site web în vederea accesării sau utilizării ofertelor IBM SaaS.

c. Date de evenimente:

   Clientul (şi un număr nelimitat de persoane care fac parte din personalul său autorizat) poate utiliza TMA pentru a primi date de evenimente generate din Software-ul Client al Titularului de Cont ca rezultat al interacţiunilor online ale Titularului de Cont cu Aplicaţia sa Business sau Retail pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS. Datele de evenimente vor fi primite de la Software-ul Client al Titularului de Cont care rulează pe dispozitivele Participanţilor Eligibili, care au acceptat EULA şi s-au autentificat cel puţin o dată în Aplicaţia Business sau Retail a Clientului, iar configuraţia Clientului trebuie să includă colectarea ID-urilor de utilizator.

d. Trusteer Splash:

   Platforma de marketing Trusteer Splash identifică şi comercializează Software-ul Client al Titularului de Cont pentru Participanţii Eligibili care accesează Aplicaţiile Business şi/sau Retail ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS. Clientul poate selecta dintre Şabloanele de Splash disponibile. Splash-ul personalizat poate fi contractat printr-un ordin de lucru sau acord separat.

Clientul poate accepta să-şi furnizeze mărcile comerciale, emblemele sau pictogramele pentru utilizarea legată de TMA şi numai pentru utilizarea cu Trusteer Splash şi pentru afişarea în Software-ul Client al Titularului de Cont sau pe paginile de întâmpinare găzduite de IBM şi pe website-ul IBM Security Trusteer. Orice utilizare a mărcilor comerciale, emblemelor sau pictogramelor sale pe care le furnizează va fi în conformitate cu politicile rezonabile IBM privind reclamele şi utilizarea mărcilor comerciale.

Clientul trebuie să se aboneze la oferta IBM Security Trusteer Rapport Mandatory Service SaaS dacă doreşte să adopte orice tip de implementare obligatorie a Software-ului Client al Titularului de Cont.

Implementarea obligatorie a Software-ului Client al Titularului de Cont include, dar nu este limitată la, orice tip de implementare obligatorie, prin orice mecanism sau mijloace, care, direct sau indirect, obligă un Participant Eligibil să descarce Software-ul Client al Titularului de Cont, sau orice metodă, instrument, procedură, acord sau mecanism care nu a fost creat sau aprobat de IBM, creat pentru a ocoli cerinţele de licenţiere ale acestei implementări obligatorii a Software-ului Client al Titularului de Cont.

2.2 Oferte IBM SaaS Suplimentare Opţionale pentru IBM Security Trusteer Rapport for Business şi/sau IBM Security Trusteer Rapport for Retail

Abonarea la ofertele IBM Security Trusteer Rapport este o cerinţă preliminară pentru abonarea la oricare dintre următoarele oferte IBM SaaS suplimentare. Dacă IBM SaaS este desemnat ca "for Business", trebuie ca şi oferta IBM SaaS suplimentară achiziţionată să fie "for Business". Dacă IBM SaaS este desemnat ca "for Retail", trebuie ca şi oferta IBM SaaS suplimentară achiziţionată să fie "for Retail". Clientul va primi datele de evenimente de la Participanţii Eligibili care rulează Software-ul Client al Titularului de Cont, au acceptat EULA şi s-au autentificat cel puţin o dată în Aplicaţiile Business şi/sau Retail ale Clientului, iar configuraţia Clientului trebuie să includă colectarea ID-urilor de utilizator.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business şi/sau IBM Security Trusteer Rapport Fraud Feeds for Retail

Clientul (şi un număr nelimitat de persoane care fac parte din personalul său autorizat) poate utiliza TMA pentru a primi date de evenimente privind infecţiile cu malware şi alte vulnerabilităţi ale punctului final pentru desktop-ul unui anumit Titular de Cont.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business şi/sau IBM Security Trusteer Rapport Phishing Protection for Retail

Clientul (şi un număr nelimitat de persoane care fac parte din personalul său autorizat) poate utiliza TMA pentru a primi notificări de date de evenimente privind trimiterea acreditărilor de logare ale Titularului de Cont către un site suspectat de phishing sau posibil fraudulos. Aplicaţiile (URL-urile) online legitime pot fi marcate în mod eronat ca site-uri de phishing şi IBM SaaS poate alerta Titularii de Cont că un site legitim este un site de phishing. Într-o astfel de situaţie, Clientul trebuie să notifice IBM despre eroare, iar IBM va corecta eroarea respectivă. Acesta va fi singurul remediu al Clientului pentru o astfel de eroare.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business şi/sau IBM Security Trusteer Rapport Mandatory Service for Retail

Clientul poate utiliza o instanţă a platformei de marketing Trusteer Splash pentru a dispune descărcarea Software-ul Client al Titularului de Cont pentru Participanţii Eligibili care accesează Aplicaţiile Business şi/sau Retail ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS.

IBM Security Trusteer Rapport Premium Support for Business este o cerinţă preliminară pentru IBM Security Rapport Mandatory Service for Business.

IBM Security Trusteer Rapport Premium Support for Retail este o cerinţă preliminară pentru IBM Security Rapport Mandatory Service for Retail.

Clientul poate implementa funcţionalitatea suplimentară IBM Security Trusteer Rapport Mandatory Service numai dacă a fost comandată şi configurată pentru utilizarea cu Aplicaţia Retail sau Business a Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS.

3. Ofertele IBM Security Trusteer Pinpoint

IBM Security Trusteer Pinpoint este un serviciu bazat pe cloud, conceput pentru furnizarea altui nivel de protecţie şi detectarea şi atenuarea efectelor atacurilor de tip malware, phishing sau preluare de cont. Trusteer Pinpoint poate fi integrat în Aplicaţiile Business şi/sau Retail ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS şi procesele de prevenire a fraudelor.

Această ofertă IBM SaaS include:

a. TMA:

   Aplicaţia TMA este făcută disponibilă în mediul găzduit în cloud IBM Security Trusteer şi permite Clientului (şi unui număr nelimitat de persoane care fac parte din personalul său autorizat): (i) primirea rapoartelor cu date de evenimente şi a evaluărilor de risc şi (ii) vizualizarea, configurarea şi setarea politicilor de securitate şi a politicilor privind raportarea datelor de evenimente.

b. Script Web şi/sau API-uri:

   Pentru implementarea pe un site web în vederea accesării sau utilizării IBM SaaS.

3.1 IBM Security Trusteer Pinpoint Malware Detection şi IBM Security Trusteer Pinpoint Criminal Detection

În eventualitatea detectării unui malware în ofertele IBM Security Trusteer Pinpoint Malware Detection sau detectării preluării contului în ofertele IBM Security Trusteer Pinpoint Criminal Detection, Clientul trebuie să urmeze indicaţiile din Pinpoint Best Practices Guide. Nu utilizaţi ofertele IBM Security Trusteer Pinpoint Malware Detection sau ofertele IBM Security Trusteer Pinpoint Criminal Detection în niciun fel care ar putea afecta experienţa Participanţilor Eligibili imediat după detectarea unui malware sau a unei preluări de cont, deoarece aceasta ar permite altora să lege acţiunile clientului cu utilizarea ofertelor IBM Security Trusteer Pinpoint (de ex. notificările, mesajele, blocarea dispozitivelor sau blocarea accesului la Aplicaţia Business şi/sau Retail imediat după detectarea unui malware sau a unei preluări de cont).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business şi/sau IBM Security Trusteer Pinpoint Criminal Detection for Retail

Detectarea fără client a unei activităţi suspecte de preluare contului în browser-ele care se conectează la o Aplicaţie Business sau Retail, utilizând ID-ul de dispozitiv, detectarea phishing-ului şi detectarea furtului de acreditări bazat pe malware. Ofertele IBM Security Trusteer Pinpoint Criminal Detection furnizează alt nivel de protecţie şi sunt axate pe detectarea tentativelor de preluare a contului şi furnizarea punctajelor de evaluare a riscului pentru browser-ele şi dispozitivele mobile (prin browser-ul nativ sau aplicaţia mobilă a clientului) care accesează o Aplicaţie Business sau Retail direct la Client.

a. Date de evenimente:

   Clientul (şi un număr nelimitat de persoane care fac parte din personalul său autorizat) poate utiliza TMA pentru a primi date de evenimente generate ca rezultat al interacţiunilor online ale Participanţilor Eligibili cu Aplicaţiile Business şi/sau Retail ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS sau Clientul poate primi datele de evenimente prin modul de livrare API backend.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile şi/sau IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

Ofertele IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) sunt concepute pentru a furniza alt nivel de protecţie şi sunt axate pe protejarea faţă de preluarea contului şi activităţile frauduloase, prin identificarea accesării ilegale a contului şi prin furnizarea unor recomandări pentru Client. Această ofertă IBM SaaS colectează informaţiile primite atât de la Aplicaţia Business şi/sau Retail a Clientului utilizând API-ul PPCD Mobile, cât şi de la dispozitivele mobile ale Participanţilor Eligibili. Ofertele IBM Security Trusteer PPCD Mobile sunt concepute pentru a corela informaţii complexe privind dispozitivele mobile ale Participanţilor Eligibili cu alte surse de date, cum ar fi incidentele în timp real de phishing sau infecţie cu malware, care sunt integrate prin alte oferte IBM SaaS ale IBM Security Trusteer's other IBM SaaS, specificate în aceşti Termeni de Utilizare.

Clientul poate accesa şi utiliza ofertele IBM Security Trusteer PPCD Mobile în mediul bazat pe cloud IBM Security Trusteer şi poate primi datele evaluărilor de risc de la dispozitivele mobile ale Participanţilor Eligibili, generate ca rezultat al interacţiunilor online ale acestor dispozitive mobile cu Aplicaţia Business sau Retail a Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS. Pentru scopul acestor oferte, "dispozitivele mobile" includ numai telefoanele mobile şi tabletele suportate, şi nu includ PC-urile sau MAC-urile.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition şi/sau IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition şi/sau IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition şi/sau IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Detectarea fără client a browser-elor care sunt infectate cu malware-ul financiar Man in the Browser (MitB) şi se conectează la o Aplicaţie Business şi/sau Retail. Ofertele IBM Security Trusteer Pinpoint Malware Detection furnizează alt nivel de protecţie şi au ca scop axarea organizaţiilor pe procesele de prevenire a fraudelor bazate pe riscul de malware, furnizând Clientului evaluări şi alerte privind prezenţa malware-ului financiar MitB.

a. Date de evenimente:

   Clientul (şi un număr nelimitat de persoane care fac parte din personalul său autorizat) poate utiliza TMA pentru a primi date de evenimente generate ca rezultat al interacţiunilor online ale Participanţilor Eligibili cu Aplicaţiile Business şi/sau Retail ale Clientului.

b. Advanced Edition:

   Advanced Editions pentru Business şi/sau Retail furnizează un nivel suplimentar de detecţie şi protecţie, care este ajustat şi personalizat pentru structura şi fluxul Aplicaţiilor Business şi/sau Retail ale Clientului şi poate fi personalizat gama de ameninţări specifice Clientului. Permite încorporarea în diverse locaţii din Aplicaţiile Business şi/sau Retail ale Clientului.

   Advanced Edition este oferit Clientului la cantităţile minime de cel puţin 100.000 Participanţi Eligibili Retail sau 10.000 Participanţi Eligibili Business, ceea ce înseamnă 1000 de pachete de câte 100 de Participanţi Eligibili pentru Retail sau 1000 de pachete de câte 10 Participanţi Eligibili pentru Business.

c. Standard Edition:

Standard Edition pentru Business sau Retail este o soluţie de implementare rapidă, care furnizează funcţionalitatea principală a cestei oferte IBM SaaS, după cum se descrie aici.

3.2 Oferte IBM SaaS suplimentare opţionale pentru IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition şi/sau IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition şi/sau IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition şi/sau IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Pentru ofertele IBM Security Trusteer Rapport Remediation for Retail, IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition sau IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition reprezintă o cerinţă preliminară.

Pentru IBM Security Trusteer Pinpoint Carbon Copy for Retail, IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition sau IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition reprezintă o cerinţă preliminară. Pentru IBM Security Trusteer Pinpoint Carbon Copy for Business, IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition sau IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition reprezintă o cerinţă preliminară.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business şi/sau IBM Security Trusteer Pinpoint Carbon Copy for Retail

Oferte IBM Security Trusteer Pinpoint Carbon Copy sunt concepute să furnizeze alt nivel de protecţie şi un serviciu de monitorizare care ajută la identificarea compromiterii acreditărilor Participantului Eligibil prin atacuri de tip phishing în Aplicaţiile Retail sau Business ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail are ca scop investigarea, remedierea, blocarea şi înlăturarea infecţiilor cu malware-ul man-in-the-browser (MitB) de pe dispozitivele (PC/MAC) infectate ale Participanţilor Eligibili ai clientului care accesează Aplicaţia Retail a Clientului, pe baza unor criterii ad-hoc, când datele de evenimente IBM Security Trusteer Pinpoint Malware Detection au detectat infecţii cu malware-ul MitB. Clientul trebuie să aibă un abonament IBM Security Trusteer Pinpoint Malware Detection în curs de derulare pentru Aplicaţia Retail a Clientului. Clientul trebuie să utilizeze această ofertă IBM SaaS numai în legătură cu Participanţii Eligibili care accesează Aplicaţia Retail a Clientului şi numai ca un instrument destinat investigării şi remedierii unui anumit dispozitiv (PC/MAC) infectat, pe baza unor criterii ad-hoc. IBM Security Trusteer Rapport Remediation for Retail trebuie să ruleze pe dispozitivul (PC/MAC) Participantului Eligibil afectat, respectivul Participant Eligibil trebuie să fi acceptat EULA şi să se fi autentificat cel puţin o dată în Aplicaţiile Retail ale Clientului, iar configuraţia Clientului trebuie să includă colectarea ID-urilor de utilizator. Pentru a se evita incertitudinile, această ofertă IBM SaaS nu include dreptul de a utiliza Trusteer Splash şi/sau de a promova Software-ul Client al Titularului de Cont în orice alt fel pentru populaţia de Participanţi Eligibili generali ai Clientului.

4. Ofertele IBM Security Trusteer Mobile

4.1 IBM Security Trusteer Mobile Browser for Business şi/sau IBM Security Trusteer Mobile Browser for Retail

IBM Security Trusteer Mobile Browser este conceput să adauge alt nivel de protecţie şi este axat pe furnizarea accesului online sigur pentru dispozitivele mobile ale Participanţilor Eligibili care accesează Aplicaţiile Retail sau Business ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS, evaluarea riscurilor dispozitivelor mobile şi protecţia anti-phishing. Detectarea comunicaţiei Wi-Fi sigure este disponibilă numai pentru platformele Android. Pentru scopul acestei oferte IBM SaaS dispozitivele mobile includ telefoanele mobile sau tabletele şi nu includ laptop-urile PC şi Mac.

Prin TMA, Clientul (şi un număr nelimitat de persoane care fac parte din personalul său autorizat) poate primi date de evenimente, analize şi informaţii statistice privind Dispozitivele ai căror Participanţi Eligibili: (i) au descărcat Software-ul Client al Titularului de Cont, o aplicaţie licenţiată gratuit pentru public în baza acordului de licenţă pentru utilizatorul final ("EULA") şi care este făcută disponibilă pentru descărcare pe dispozitivele mobile ale Participanţilor Eligibile şi (ii) au acceptat EULA şi s-au autentificat cel puţin o dată în Aplicaţiile Business sau Retail ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM

SaaS. Clientul poate doar să comercializeze Software-ul Client al Titularului de Cont utilizând Trusteer Splash şi nu poate utiliza Software-ul Client al Titularului de Cont pentru operaţiile sale interne de afaceri.

a. Date de evenimente:

   Clientul (şi un număr nelimitat de persoane care fac parte din personalul său autorizat) poate utiliza TMA pentru a primi date de evenimente generate ca rezultat al interacţiunilor online ale dispozitivelor mobile cu Aplicaţiile Retail sau Business ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS.

b. Trusteer Splash:

   Platforma de marketing Trusteer Splash identifică şi comercializează Software-ul Client al Titularului de Cont pentru Participanţii Eligibili care accesează Aplicaţiile Business şi/sau Retail ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS. Clientul poate selecta dintre şabloanele de splash disponibile ("Şabloanele de Splash"). Splash-ul personalizat poate fi contractat printr-un ordin de lucru sau acord separat.

Clientul poate accepta să-şi furnizeze mărcile comerciale, emblemele sau pictogramele pentru utilizarea legată de TMA şi numai pentru utilizarea cu Trusteer Splash şi pentru afişarea în Software-ul Client al Titularului de Cont sau pe paginile de întâmpinare găzduite de IBM, sau pe website-ul IBM Security Trusteer. Orice utilizare a mărcilor comerciale, emblemelor sau pictogramelor sale pe care le furnizează va fi în conformitate cu politicile rezonabile IBM privind reclamele şi utilizarea mărcilor comerciale.

4.2 IBM Security Trusteer Mobile SDK for Business şi/sau IBM Security Trusteer Mobile SDK for Retail

Ofertele IBM Security Trusteer Mobile SDK sunt concepute pentru a adăuga alt nivel de protecţie, pentru a furniza un acces web sigur la Aplicaţiile Business şi/sau Retail ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS, evaluarea riscurilor dispozitivelor mobile şi protecţia anti-pharming. Detectarea comunicaţiei Wi-Fi sigure este disponibilă numai pentru platformele Android.

Ofertele IBM Security Trusteer Mobile SDK includ un kit de proprietar pentru dezvoltarea software-ului mobil ("SDK"), un pachet software ce conţine documentaţia, bibliotecile de software de proprietar pentru programare şi alte fişiere şi articole conexe, numite biblioteca mobilă IBM Security Trusteer, precum şi "Componenta Runtime", sau "Redistribuibilul", un cod de proprietar generat de IBM Security Trusteer Mobile SDK ce poate fi înglobat şi integrat în aplicaţiile mobile iOS sau Android autonome şi protejate ale Clientului pentru care Clientul s-a abonat la acoperirea ofertelor IBM SaaS ("Aplicaţia Mobilă Integrată a Clientului").

IBM Security Trusteer Mobile SDK for Retail este disponibil în pachete de 100 de Participanţi Eligibili sau pachete de 100 de Dispozitive Client, iar IBM Security Trusteer Mobile SDK for Business este disponibil în pachete de 10 Participanţi Eligibili sau pachete de 10 de Dispozitive Client.

Prin TMA, Clientul (şi un număr nelimitat de persoane care fac parte din personalul său autorizat) poate primi raportări ale datelor de eveniment şi evaluări ale tendinţelor riscului. Prin Aplicaţia Mobilă Integrată a Clientului, Clientul poate primi analize de risc şi informaţii privind dispozitivele mobile ale Participanţilor Eligibili care au descărcat Aplicaţia Mobilă Integrată a Clientului, astfel încât Clientul poate formula o politică de prevenire a fraudelor, care să impună acţiuni pentru diminuarea riscurilor respective. Pentru scopul acestei oferte, "dispozitivele mobile" includ numai telefoanele mobile şi tabletele suportate, şi nu includ PC-urile sau MAC-urile.

Clientul poate:

a. să utilizeze intern IBM Security Trusteer Mobile SDK numai în scopul dezvoltării Aplicaţiei Mobile Integrate a Clientului;

b. să înglobeze Redistribuibilul (numai în format cod obiect), ca o modalitate integrală, inseparabilă, în Aplicaţia Mobilă Integrată a Clientului. Orice porţiune din Redistribuibil modificată sau combinată în baza acestei licenţe va face obiectul acestor Termeni de Utilizare; şi

c. să comercializeze şi să distribuie Redistribuibilul pentru descărcarea pe dispozitivele mobile ale Participanţilor Eligibili sau la deţinătorul Dispozitivului Client, cu condiţia ca:

   - Cu excepţia celor permise în mod expres de acest Contract, Clientul (1) nu poate utiliza, copia, modifica sau distribui SDK-ul; (2) nu poate dezasambla, decompila, translata în alt fel sau utiliza ingineria inversă asupra SDK-ului, cu excepţia cazurilor permise în mod expres de lege, fără posibilitatea de renunţare contractuală; (3) nu poate sublicenţia, închiria sau da în leasing SDK-ul; (4) nu poate înlătura niciun fişier de copyright sau anunţ inclus în

Redistribuibil; (5) nu poate utiliza acelaşi nume de cale ca fişierele/modulele Redistribuibilului original; şi (6) nu poate utiliza numele sau mărcile comerciale deţinute de IBM, licenţiatorii sau distribuitorii săi, în legătură cu comercializarea Aplicaţiei Mobile Integrate a Clientului, fără consimţământul acordat în prealabil de IBM sau de licenţiatorul sau distribuitorul său.

- Redistribuibilul trebuie să rămână integrat, într-o modalitate care să nu permită separarea, în Aplicaţia Mobilă Integrată a Clientului. Redistribuibilul trebuie să fie numai în format cod obiect şi să respecte toate indicaţiile, instrucţiunile şi specificaţiile din SDK şi documentaţia sa. Acordul de licenţă cu utilizatorul final pentru Aplicaţia Mobilă Integrată a Clientului trebuie să notifice utilizatorul final că Redistribuibilul i) nu poate fi utilizat pentru alt scop decât activarea Aplicaţiei Mobile Integrate a Clientului ii) nu poate fi copiat (exceptând scopurile legate de backup), iii) nu poate fi distribuit sau transferat, iv) nu poate fi dezasamblat, decompilat sau translatat în alt fel, decât după cum este permis expres de lege şi fără posibilitatea de renunţare contractuală. Acordul de licenţă al Clientului trebuie să asigure pentru IBM un nivel de protecţie cel puţin egal cu cel al termenilor din acest Contract.
- SDK-ul poate fi implementat numai ca parte a dezvoltării interne şi testării unităţilor Clientului, pe dispozitivele mobile ale Clientului specificate pentru testare. Clientul nu este autorizat să utilizeze SDK-ul pentru procesarea încărcărilor de lucru destinate producţiei, simularea încărcărilor de lucru de producţie sau testarea scalabilităţii oricărui cod, aplicaţii sau sistem. Clientul nu este autorizat să utilizeze nicio parte a SDK-ului, indiferent de scop.

Clientul este responsabil pentru întreaga asistenţă tehnică pentru Aplicaţia Mobilă Integrată a Clientului şi pentru orice modificări aduse Redistribuibilelor de către Client, după cum se permite aici.

Clientul este autorizat să instaleze şi să utilizeze Redistribuibilele şi IBM Security Mobile SDK numai ca suport pentru utilizarea de către Client a ofertei IBM SaaS.

IBM a testat aplicaţiile eşantion create cu instrumentele mobile furnizate în IBM Security Trusteer Mobile SDK ("Instrumentele Mobile"), pentru a determina dacă ele se vor executa corespunzător pe anumite versiuni de platforme pentru sisteme de operare mobile de la Apple (iOS), Google (Android) şi de la alţii (numite colectiv "Platforme pentru Sisteme de Operare Mobile"), însă Platformele pentru Sisteme de Operare Mobile sunt furnizate de terţe părţi, nu sunt controlate de IBM şi pot suferi modificări fără ca IBM să fie notificat. Ca urmare, şi fără a ţine cont de nicio prevedere contrară, IBM nu garantează că aplicaţiile sau alte ieşiri create cu Instrumentele Mobile se vor executa corespunzător pe, vor interopera cu sau vor fi compatibile cu orice Platforme pentru Sisteme de Operare Mobile sau dispozitive mobile.

Clientul este de acord să creeze, să păstreze şi să furnizeze către IBM şi auditorii săi înregistrări scrise precise, ieşirile instrumentelor de sistem şi alte informaţii despre sistem, suficiente pentru a se putea verifica prin audit dacă utilizarea de către Client a IBM Security Trusteer Mobile SDK este conformă cu aceşti Termeni de Utilizare.

5. Implementarea Ofertelor IBM SaaS Fraud Protection

Abonamentul de bază al Clientului include setarea necesară şi activităţile iniţiale de implementare, cum ar fi pornirea iniţială unică, configurarea, Şablonul de Splash, testarea şi instruirea.

Pot fi contractate şi alte servicii, pentru un tarif suplimentar, în baza unui contract separat.

Anexa B

IBM furnizează următorul acord privind nivelul serviciilor ("SLA") pentru IBM SaaS, acesta fiind aplicabil dacă este specificat în Documentul Tranzacţional al Clientului:

Se va aplica versiunea acestui SLA care este în vigoare la începerea sau reînnoirea abonamentului Clientului. Clientul înţelege că SLA-ul nu constituie o garanţie pentru Client.

1. Definiţii

a. **Contact Autorizat** – înseamnă persoana pe care Clientul a specificat-o la IBM ca fiind autorizată să trimită Reclamaţii în baza acestui SLA.

b. **Credit de Disponibilitate** – înseamnă remediul pe care IBM îl furnizează pentru o Reclamaţie validată. Creditul de Disponibilitate va fi aplicat sub formă de credit sau reducere pentru o viitoare factură, cu tariful de abonare la IBM SaaS.

c. **Reclamaţie** – înseamnă o reclamaţie trimisă la IBM de către Contactul Autorizat al Clientului, ca urmare a neîndeplinirii unui Nivel de Serviciu din acest SLA într-o Lună Contractată.

d. **Lună Contractată** – înseamnă fiecare lună întreagă a duratei termenului IBM SaaS, măsurată de la 00:00 GMT în prima zi a lunii până la 23:59 GMT în ultima zi a lunii.

e. **Client** – înseamnă o entitate care se abonează pentru IBM SaaS direct la IBM şi care nu este în culpă privind îndeplinirea unor obligaţii substanţiale, inclusiv obligaţii de plată, care decurg din contractul său cu IBM pentru IBM SaaS.

f. **Timp de Nefuncţionare** – înseamnă perioada în care sistemul de producţie care lucrează pentru Servicii a fost oprit şi utilizatorii nu mai pot utiliza toate aspectele Serviciului pentru care au permisiuni corespunzătoare. Timpul de Nefuncţionare nu include perioada în care indisponibilitatea Serviciului este cauzată de:

- Timpul Planificat de Nefuncţionare a Sistemului;
- Forţă Majoră;
- Probleme legate de aplicaţiile, echipamentul sau datele Clientului sau ale unei terţe părţi;
- Acţiuni sau omisiuni ale Clientului sau ale unei terţe părţi (inclusiv ale oricărei persoane care obţine acces la IBM SaaS prin intermediul parolelor sau echipamentului Clientului);
- Nerespectarea cerinţelor privind configuraţiile de sistem necesare şi platformele suportate pentru accesarea IBM SaaS; sau
- Conformitatea IBM cu orice proiecte, specificaţii sau instrucţiuni furnizate de Client sau de o terţă parte în numele Clientului

g. **Eveniment** – înseamnă situaţia sau setul de situaţii considerate împreună, care determină neîndeplinirea unui Nivel de Serviciu.

h. **Forţă Majoră** – înseamnă un eveniment neprevăzut, act de terorism, acţiune sindicală, incendiu, inundaţie, cutremur, revoltă, război, hotărâri guvernamentale, ordine sau restricţii, viruşi, atacuri de tip refuzul serviciului (denial of service) sau de alt fel, defecţiuni privind utilităţile şi conectivitatea reţelei sau orice altă cauză a indisponibilităţii IBM SaaS care a fost în afara controlului rezonabil al IBM.

i. **Timp Planificat de Nefuncţionare a Sistemului** – înseamnă o întrerupere planificată a IBM SaaS în scopul mentenanţei.

j. **Nivel de Serviciu** – înseamnă standardul stabilit mai jos, utilizat de IBM pentru a măsura nivelul serviciului furnizat în baza acestui SLA.

2. Credite de Disponibilitate

a. Pentru a putea trimite o Reclamaţie, Clientul trebuie să fi înregistrat un tichet de suport pentru fiecare Eveniment, la Help Desk-ul de suport pentru clienţii IBM pentru oferta IBM SaaS aplicabilă, conform procedurii IBM de raportare a problemelor de Severitate 1. Clientul trebuie să furnizeze toate detaliile necesare cu privire la Eveniment şi să asigure personalului IBM o asistenţă rezonabilă pentru diagnosticarea şi rezolvarea Evenimentului, în măsura cerută pentru tichetele de

suport de Severitate 1. Un astfel de tichet trebuie să fie înregistrat într-un interval de douăzeci şi patru (24) de ore de la momentul în care Clientul a sesizat că Evenimentul afectează utilizarea sa IBM SaaS.

b. Pentru a obţine un Credit de Disponibilitate, Contactul Autorizat al Clientului trebuie să trimită Reclamaţia Clientului nu mai târziu de trei (3) zile lucrătoare după terminarea Lunii Contractate care face obiectul Reclamaţiei.

c. Contactul Autorizat al Clientului trebuie să furnizeze către IBM toate detaliile rezonabile privind Reclamaţia, incluzând, dar fără a se limita la, descrierile detaliate ale tuturor Evenimentelor relevante şi Nivelul de Serviciu care a fost reclamat ca neîndeplinit.

d. IBM va măsura intern Timpul de Nefuncţionare total combinat din fiecare Lună Contractată aplicabil pentru Nivelul de Serviciu corespondent afişat în tabelul de mai jos. Creditele de Disponibilitate vor fi bazate pe Timpul de Nefuncţionare măsurat începând cu momentul în care Clientul a raportat prima dată impactul Timpului de Nefuncţionare. În cazul în care Clientul raportează simultan un Eveniment de Timp de Nefuncţionare Aplicaţie şi un Eveniment de Timp de Nefuncţionare Procesare Date de Intrare, IBM va trata intervalele suprapuse de Timp de Nefuncţionare ca un singur interval de Timp de Nefuncţionare, nu ca intervale separate de Timp de Nefuncţionare. Pentru fiecare Reclamaţie validă, IBM va aplica cel mai înalt Credit de Disponibilitate aplicabil pe baza Nivelului de Serviciu obţinut în fiecare Lună Contractată, aşa cum se arată în tabelele de mai jos. IBM nu va fi răspunzător pentru mai multe Credite de Disponibilitate pentru aceleaşi Evenimente în aceeaşi Lună Contractată.

e. În cazul unui Serviciu Bundle (oferte IBM SaaS individuale împachetate şi vândute împreună cu un preţ combinat unic), Creditul de Disponibilitate va fi calculat pe baza preţului lunar combinat unic al Serviciului Bundle, nu pe baza tarifului lunar de abonare la fiecare IBM SaaS individual. Clientul poate trimite numai Reclamaţii referitoare la un IBM SaaS individual dintr-un bundle, în oricare Lună Contractată, iar IBM nu va fi răspunzător pentru Creditele de Disponibilitate privind mai multe oferte IBM SaaS dintr-un bundle, în oricare Lună Contractată.

f. În cazul în care Clientul a cumpărat IBM SaaS de la un revânzător IBM valid printr-o tranzacţie de remarketing în care IBM deţine principala responsabilitate pentru livrarea IBM SaaS şi angajamentele din SLA, Creditul de Disponibilitate va fi bazat pe preţul RSVP (Relationship Suggested Value Price) din acel moment pentru oferta IBM SaaS efectivă pentru Luna Contractată care face obiectul Reclamaţiei, cu o reducere de 50%.

g. Totalul Creditelor de Disponibilitate acordate pentru orice Lună Contractată nu va depăşi în nicio situaţie zece procente (10%) din a douăsprezecea parte (1/12) a tarifului anual plătit de Client către IBM pentru IBM SaaS.

h. IBM va utiliza criterii rezonabile de validare a Reclamaţiei, pe baza informaţiilor disponibile în înregistrările IBM, care vor prevala în eventualitatea unui conflict cu datele din înregistrările Clientului.

i. CREDITELE DE DISPONIBILITATE CARE SUNT FURNIZATE CLIENTULUI ÎN CONFORMITATE CU ACEST SLA REPREZINTĂ REMEDIUL UNIC ŞI EXCLUSIV PENTRU ORICE RECLAMAŢIE A CLIENTULUI.

3. Nivelurile de Serviciu

Disponibilitatea IBM SaaS într-o Lună Contractată

Nivelul de Serviciu Realizat (pe durata unei Luni Contractate)	**Credit de Disponibilitate (% din Tariful de Abonare Lunar pentru Luna Contractată care face obiectul Reclamaţiei)**
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

"Nivelul de Serviciu Realizat", exprimat ca procentaj, este calculat astfel: (a) numărul total de minute dintr-o Lună Contractată minus (b) numărul total de minute de Timp de Nefuncţionare într-o Lună Contractată, împărţit la (c) numărul total de minute dintr-o Lună Contractată.

Exemplu: Un total de 250 de minute Timp de Nefuncţionare într-o Lună Contractată

43.200 minute într-o Lună Contractată de 30 de zile - 250 de minute Timp de Nefuncţionare = 42.950 minute _____ 43.200 de minute în total	= 2% Credit de Disponibilitate pentru Nivelul de Serviciu Realizat de 99,4% în Luna Contractată

3.1 Excluderi

Acest SLA este disponibil numai pentru Clienţii IBM. Acest SLA nu se aplică pentru următoarele:

- Servicii beta şi trial.
- Mediile care nu sunt de producţie, incluzând, dar fără a se limita la, mediile de testare, de recuperare după un dezastru, de asigurare a calităţii sau de dezvoltare.
- Reclamaţii făcute de către utilizatorii, vizitatorii, participanţii şi invitaţii permişi ai unui Client IBM pentru IBM SaaS.
- Cazurile în care Clientul nu şi-a îndeplinit o obligaţie substanţială prevăzută de Termenii de Utilizare, incluzând, dar fără a se limita la, neîndeplinirea oricărei obligaţii privind plata.