IBM Security Trusteer Fraud Protection

De Gebruiksvoorwaarden ("ToU") bestaan uit deze IBM Gebruiksvoorwaarden – SaaS Specifieke Voorwaarden voor Aanbieding ("SaaS Specifieke Voorwaarden voor Aanbieding") en een document met de titel IBM Gebruiksvoorwaarden – Algemene bepalingen ("Algemene Voorwaarden") dat beschikbaar is op de volgende URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

In geval van tegenstrijdigheid prevaleren de SaaS Specifieke Voorwaarden voor Aanbieding boven de Algemene Voorwaarden. Door de IBM SaaS te bestellen, te openen of te gebruiken, geeft Klant aan akkoord te gaan met deze Gebruiksvoorwaarden.

De Gebruiksvoorwaarden worden beheerst door de IBM International Passport Advantage Overeenkomst, de IBM International Passport Advantage Express Overeenkomst of de IBM International Agreement for Selected IBM SaaS Offerings, zoals van toepassing ("Overeenkomst") en vormen samen met de Gebruiksvoorwaarden de volledige overeenkomst.

1. IBM SaaS

De volgende IBM SaaS-aanbiedingen worden gedekt door deze SaaS Specifieke Voorwaarden voor Aanbieding:

1.1 Rapport IBM SaaS-aanbiedingen

- 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 Pinpoint IBM SaaS-aanbiedingen

- 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 Mobile IBM SaaS-aanbiedingen

- 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. Maateenheden voor verschuldigde bedragen

De IBM SaaS wordt verkocht onder een van de volgende maateenheden voor verschuldigde bedragen, zoals gespecificeerd in het Transactiedocument:

a. **In Aanmerking Komende Deelnemer** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Elke persoon of entiteit die in aanmerking komt om deel te nemen aan welk door de IBM SaaS beheerd of getraceerd servicedeliveryprogramma dan ook, is een In Aanmerking Komende Deelnemer. Er dienen voldoende gebruiksrechten te worden verworven ter dekking van alle In Aanmerking Komende Deelnemers die binnen de IBM SaaS worden beheerd of getraceerd tijdens de meetperiode zoals aangegeven in het Transactiedocument van Klant.

Elk servicedeliveryprogramma dat door de IBM SaaS wordt beheerd, wordt afzonderlijk geanalyseerd en vervolgens samengevoegd. Voor personen of entiteiten die in aanmerking komen voor meerdere servicedeliveryprogramma's zijn er afzonderlijke gebruiksrechten vereist.

Voor deze aanbiedingen geldt dat een servicedeliveryprogramma een enkele Business of Retail Applicatie van Klant omvat, met een hoofd-aanmeldingspagina en aanverwante pagina's voor elke Business of Retail Applicatie. Een In Aanmerking Komende Deelnemer is een eindgebruiker van Klant, voor wie er legitimatiegegevens voor aanmelding bij de Business of Retail Applicatie bestaan.

b. **Clientapparaat** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Een Clientapparaat is een apparaat voor computergebruik, een sensor voor speciale doeleinden of een apparaat voor telemetrie voor een enkele gebruiker, dat verzoekt om de uitvoering van een set van opdrachten, procedures of applicaties of dat deze ontvangt voor uitvoering, of dat gegevens verstrekt aan een ander computersysteem waarnaar in het algemeen wordt verwezen als een server of dat anderszins wordt beheerd door de server. Meerdere Clientapparaten kunnen toegang hebben tot een gemeenschappelijke server. Een Clientapparaat kan over een bepaalde hoeveelheid verwerkingskracht beschikken of kan zodanig te programmeren zijn, dat een gebruiker er werk op kan uitvoeren. Klant dient gebruiksrechten te verkrijgen voor elk Clientapparaat dat de IBM SaaS uitvoert, er gegevens aan verstrekt, services gebruikt die erdoor worden verstrekt, of er anderszins toegang toe heeft, om tijdens de meetperiode zoals aangegeven in het Transactiedocument van Klant, gebruik te mogen maken van de IBM SaaS.

3. Verschuldigde bedragen en facturering

Het verschuldigde bedrag voor de IBM SaaS wordt aangegeven in een Transactiedocument.

3.1 Verschuldigd bedrag voor een deel van een maand

Voor een deel van een maand kunnen er pro rato verschuldigde bedragen in rekening worden gebracht, zoals gespecificeerd in het Transactiedocument.

4. Naleving en controle

Voor de toegang tot IBM Security Trusteer Fraud Protection aanbiedingen geldt een maximum aantal In Aanmerking Komende Deelnemers of Clientapparaten zoals gespecificeerd in het Transactiedocument. Het is de verantwoordelijkheid van Klant te garanderen dat zijn aantal In Aanmerking Komende Deelnemers of Clientapparaten het in het Transactiedocument gespecificeerde maximum aantal niet overschrijdt.

Er kan een audit worden uitgevoerd om te controleren of het maximum aantal In Aanmerking Komende Deelnemers of Clientapparaten niet wordt overschreden.

5. Opties voor verlenging van de Abonnementsperiode voor IBM SaaS

In het Transactiedocument van Klant wordt, door de Abonnementsperiode aan te merken als een van de volgende, aangegeven of de IBM SaaS aan het eind van de Abonnementsperiode wordt verlengd:

5.1 Automatische verlenging

Indien het Transactiedocument van Klant aangeeft dat de verlenging automatisch plaatsvindt, kan Klant een vervallende Abonnementsperiode van de IBM SaaS beëindigen op schriftelijk verzoek aan de IBM-vertegenwoordiger of IBM Business Partner van Klant, ten minste negentig (90) dagen vóór de vervaldatum die is aangegeven in het Transactiedocument. Indien noch IBM, noch zijn IBM Business Partner op de vervaldatum een dergelijk beëindigingsverzoek heeft ontvangen, wordt de aflopende Abonnementsperiode automatisch verlengd, hetzij met één jaar, hetzij voor dezelfde duur als de oorspronkelijke Abonnementsperiode, zoals aangegeven in het Transactiedocument.

5.2 Doorlopende facturering

Indien in het Transactiedocument wordt aangegeven dat de verlenging van Klant doorlopend plaatsvindt, blijft Klant toegang houden tot de IBM SaaS en blijft Klant op basis van doorlopende verlenging gefactureerd worden voor het gebruik van de IBM SaaS. Om het gebruik van de IBM SaaS te beëindigen en het doorlopende factureringsproces te doen stoppen, dient Klant IBM of zijn IBM Business Partner op een termijn van negentig (90) dagen schriftelijk te verzoeken de IBM SaaS te annuleren. Na annulering van de toegang van Klant wordt Klant gefactureerd voor alle uitstaande bedragen voor toegang, tot en met de maand waarin de annulering van kracht werd.

5.3 Verlenging noodzakelijk

Indien in het Transactiedocument wordt aangegeven dat het type verlenging "beëindiging" is, wordt de IBM SaaS aan het eind van de Abonnementsperiode beëindigd en wordt de toegang van Klant tot de IBM SaaS ingetrokken. Teneinde de IBM SaaS na deze einddatum te blijven gebruiken, dient Klant bij zijn IBM-verkoper of IBM Business Partner een bestelling voor de aankoop van een nieuwe Abonnementsperiode te plaatsen.

6. Technische ondersteuning

Voor Klant en diens In Aanmerking Komende Deelnemers is er Technische Ondersteuning voor de IBM SaaS beschikbaar om hen te helpen bij het werken met de IBM SaaS.

Standard Support is inbegrepen in het abonnement op alle aanbiedingen. Voor Trusteer Rapport Mandatory Service, een add-on voor Trusteer Rapport, geldt Premium Support voor het basisabonnement op Trusteer Rapport als voorwaarde.

Voor elke IBM SaaS-aanbieding, met uitzondering van IBM Security Trusteer Mobile SDK-aanbiedingen en IBM Security Trusteer Rapport Mandatory Service-aanbiedingen, is er voor een aanvullend bedrag een abonnement op Premium Support verkrijgbaar.

Standard Support:

- Ondersteuning van 8:00 - 17:00 uur lokale tijd.
- Klanten en hun In Aanmerking Komende Deelnemers kunnen op elektronische wijze tickets indienen, zoals uiteengezet in het Software as a Service [SaaS] Support Handbook.
- Klanten kunnen voor mededelingen, documenten, zaakrapporten en veelgestelde vragen terecht op de Client Support Portal, op: http://www-01.ibm.com/software/security/trusteer/support/.
- Voor gegevens en mogelijkheden inzake ondersteuning kunnen Klanten het IBM Software as a Service [SaaS] Support Handbook raadplegen: http://www-01.ibm.com/software/support/handbook.html.

Premium Support:

- 24x7 ondersteuning voor alle severity's.
- Klanten hebben rechtstreeks telefonische toegang tot ondersteuning.
- Klanten en hun In Aanmerking Komende Deelnemers kunnen op elektronische wijze tickets indienen, zoals uiteengezet in het Software as a Service [SaaS] Support Handbook.
- Klanten kunnen voor mededelingen, documenten, zaakrapporten en veelgestelde vragen terecht op de Client Support Portal, op: http://www-01.ibm.com/software/security/trusteer/support/.
- Voor gegevens en mogelijkheden inzake ondersteuning kunnen Klanten het IBM Software as a Service [SaaS] Support Handbook raadplegen: http://www-01.ibm.com/software/support/handbook.html.

7. Aanvullende bepalingen voor IBM SaaS-aanbiedingen

7.1 Naleving van Safe Harbor

IBM houdt zich aan het door het Amerikaanse Ministerie van Handel in samenwerking met de Europese Commissie ontwikkelde Amerikaans – Europese (EU) Safe Harbor Framework. IBM Security Trusteer-producten maken deel uit van de Amerikaans-Europese (EU) Safe Harbor-certificering van IBM. Meer informatie over Safe Harbor en de lijst van Safe Harbor-bedrijven is te vinden op http://export.gov/safeharbor/.

7.2 Jaarlijkse verhoging van het abonnementsbedrag van Klant

IBM behoudt zich het recht voor om het abonnementsbedrag voor de IBM SaaS, niet vaker dan eens per twaalf (12) maanden, te verhogen met een door IBM bepaald percentage van maximaal 3%. De aanpassing van het abonnementsbedrag wordt van kracht op de verjaardatum van de begindatum van de initiële dekkingsperiode. Deze aanpassing van het abonnementsbedrag heeft geen gevolgen voor de rechten van Klant op de IBM SaaS, noch voor de maateenheid voor facturering waaronder de IBM SaaS is verkregen. IBM Business Partners zijn onafhankelijk van IBM en zij stellen hun prijzen en voorwaarden eenzijdig vast.

7.3 Premium Support

Klant heeft uitsluitend recht op Premium Support voor IBM SaaS-aanbiedingen waarvoor Klant zich heeft geabonneerd op de bijbehorende Premium Support-aanbieding.

7.4 Wettig gebruik en toestemming

Toestemming voor het verzamelen en verwerken van gegevens

De IBM SaaS is ontworpen om Klant te helpen zijn beveiligingsomgeving en -gegevens te verbeteren. De IBM SaaS verzamelt informatie van de In Aanmerking Komende Deelnemers en Clientapparaten die interactief werken met de Business of Retail Applicaties waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen. De IBM SaaS verzamelt informatie die in bepaalde rechtsgebieden op zichzelf of gecombineerd kan worden beschouwd als Persoonsgegevens. Persoonsgegevens zijn: alle informatie die kan worden gebruikt om een specifiek individu te specificeren, zoals een naam, e-mailadres, thuisadres of telefoonnummer, die ter opslag, verwerking of overdracht namens Klant aan IBM wordt verstrekt.

De werkwijzen voor het verzamelen en verwerken van gegevens kunnen worden gewijzigd teneinde de functionaliteit van de IBM SaaS te verbeteren. Een document waarin de werkwijzen voor het verzamelen en verwerken van gegevens uitvoerig worden beschreven, wordt waar nodig bijgewerkt en wordt op verzoek ter beschikking gesteld aan Klant. Klant geeft IBM toestemming voor het verzamelen van deze

informatie en het verwerken ervan overeenkomstig de artikelen Overschrijding van landsgrenzen en Bescherming van persoonsgegevens van deze Gebruiksvoorwaarden, en het artikel Gegevensbescherming en -beveiliging van de Gebruiksvoorwaarden - Algemene bepalingen.

Voor IBM Security Trusteer Pinpoint-aanbiedingen:

Tot de verzamelde gegevens kunnen behoren: IP-adres van gebruiker, versleuteld of in één richting gehasht gebruikers-ID, domeincookies indien niet gefilterd, bezoeken aan beschermde Applicaties en phishingsites, geografische locatie en op phishingsites ingevoerde legitimatiegegevens.

Voor IBM Security Trusteer Mobile SDK-aanbiedingen en IBM Security Trusteer Mobile Browser-aanbiedingen:

Tot de verzamelde gegevens kunnen behoren: IP-adres van gebruiker, versleuteld of in één richting gehasht gebruikers-ID, en bezoeken aan beschermde Applicaties, SIM-kaartgegevens, apparaatnaam en banden met klant.

Voor IBM Security Trusteer Rapport-aanbiedingen:

Tot de verzamelde gegevens kunnen behoren: IP-adres van gebruiker, versleuteld of in één richting gehasht gebruikers-ID, beveiligingsevents, gebruikersnaam of e-mailadres verstrekt voor het opnemen van contact met IBM voor klantenondersteuning, banden met klant, versleutelde wachtwoorden ingevoerd op beschermde sites, bezoeken aan beschermde Applicaties en phishingsites, versleutelde betaalkaartnummers, en bestanden en gegevens die op afstand door IBM-personeel zijn verzameld ten behoeve van het onderzoeken van vermoedelijke malware, kwaadaardige activiteiten of storingen.

Op de juiste informatie gebaseerde toestemming van betrokkenen:

Bij het gebruik van deze IBM SaaS kunnen diverse wetten en regelingen betrokken zijn. De IBM SaaS mag uitsluitend op wettige wijze worden gebruikt en uitsluitend voor wettige doeleinden. Klant verklaart bij het gebruik van de IBM SaaS alle toepasselijke wetten, regelingen en beleidslijnen te zullen naleven en volledig verantwoordelijk te zijn voor deze naleving.

Voor IBM Security Trusteer Pinpoint-aanbiedingen en voor IBM Security Trusteer Mobile SDK-aanbiedingen:

Klant verklaart de op de juiste informatie gebaseerde toestemmingen, machtigingen of vergunningen te hebben verkregen en te zullen verkrijgen om wettig gebruik van de IBM SaaS mogelijk te maken en om het verzamelen en verwerken van de informatie door IBM via de IBM SaaS te rechtvaardigen.

Voor IBM Security Trusteer Rapport-aanbiedingen en voor IBM Security Trusteer Mobile Browser-aanbiedingen:

Klant geeft IBM toestemming om de op de juiste informatie gebaseerde toestemmingen te verkrijgen zoals vereist om het wettig gebruik van he IBM SaaS mogelijk te maken en om de informatie te verzamelen en te verwerken zoals beschreven in de End User License Agreement die beschikbaar is op https://www.trusteer.com/support/end-user-license-agreement. In geval Klant besluit zelf de communicatie met eindgebruikers inzake toestemming op zich te nemen (en dit dus niet over te laten aan IBM), verklaart Klant de op de juiste informatie gebaseerde toestemmingen, machtigingen of vergunningen te hebben verkregen of te zullen verkrijgen om wettig gebruik van de IBM SaaS mogelijk te maken en om het verzamelen en verwerken van de informatie door IBM als gegevensverwerker van Klant via de IBM SaaS te rechtvaardigen.

7.5 Overschrijding van landsgrenzen

Klant gaat ermee akkoord dat IBM de content, met inbegrip van Persoonsgegevens, onder de toepasselijke wet- en regelgeving over landsgrenzen heen mag verplaatsen naar verwerkers en subverwerkers in de volgende landen buiten het Europees Economisch Gebied en landen waarvan het beschermingsniveau door de Europese Commissie is aangemerkt als voldoende: de Verenigde Staten van Amerika.

7.6 Bescherming van persoonsgegevens

Indien Klant in de Lidstaten van de EU, IJsland, Liechtenstein, Noorwegen of Zwitserland Persoonsgegevens beschikbaar stelt aan de IBM SaaS, of inden Klant In Aanmerking Komende Deelnemers of Clientapparaten in die landen heeft, dan stelt Klant, als enige voor de verwerking verantwoordelijke, IBM aan als verwerker voor het verwerken (zoals deze termen zijn gedefinieerd in EU Richtlijn 95/46/EC) van Persoonsgegevens. IBM zal dergelijke Persoonsgegevens slechts verwerken voor zover noodzakelijk voor het beschikbaar stellen van IBM SaaS-aanbiedingen overeenkomstig IBM's

gepubliceerde beschrijvingen van IBM SaaS, en Klant verklaart dat dergelijke verwerking strookt met de instructies van Klant. IBM zal Klant naar redelijkheid vooraf in kennis stellen indien IBM wezenlijke wijzigingen aanbrengt in de verwerkingslocatie of in de manier waarop Persoonsgegevens door IBM worden beveiligd als onderdeel van IBM SaaS. Klant kan de lopende Abonnementsperiode voor de desbetreffende IBM SaaS beëindigen door binnen dertig (30) dagen na IBM's kennisgeving van de wijziging aan Klant, schriftelijk op te zeggen bij IBM. Klant gaat ermee akkoord dat IBM content, met inbegrip van Persoonsgegevens, ter verwerking over landsgrenzen heen mag verplaatsen naar de volgende verwerkers en subverwerkers:

Naam verwerker/subverwerker	Rol (gegevensverwerker of subverwerker)	Locatie*
De opdrachtgevende IBM-entiteit	Verwerker	Zoals aangegeven op het Transactiedocument
Amazon Web Services LLC	Subverwerker	410 Terry Ave. N Seattle, WA 98109 Verenigde Staten
Connectria Corp.	Subverwerker	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 Verenigde Staten
IBM Israel Ltd.	Subverwerker	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israël
IBM Corp	Subverwerker	1 New Orchard Rd. Armonk, NY 10504 Verenigde Staten

Klant gaat ermee akkoord dat IBM deze lijst van landen na voorafgaand bericht kan aanpassen wanneer IBM dit naar redelijkheid noodzakelijk acht voor het leveren van de IBM SaaS.

Voor service die via het Duitse datacenter wordt verleend, zoals bepaald tijdens het provisioningproces, gaat Klant ermee akkoord dat IBM content, met inbegrip van Persoonsgegevens, ter verwerking over landsgrenzen heen mag verplaatsen naar de volgende verwerkers en subverwerkers:

Naam verwerker/subverwerker	Rol (gegevensverwerker of subverwerker)	Locatie*
De opdrachtgevende IBM-entiteit	Verwerker	Zoals aangegeven op het Transactiedocument
Amazon Web Services (Duitsland)	Subverwerker	München
IBM Israel Ltd.	Subverwerker	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israël

Voor service die via het Japanse datacenter wordt verleend, zoals bepaald tijdens het provisioningproces, gaat Klant ermee akkoord dat IBM content, met inbegrip van Persoonsgegevens, ter verwerking over landsgrenzen heen mag verplaatsen naar de volgende verwerkers en subverwerkers:

Naam verwerker/subverwerker	Rol (gegevensverwerker of subverwerker)	Locatie*
De opdrachtgevende IBM-entiteit	Verwerker	Zoals aangegeven op het Transactiedocument
Amazon Web Services (Japan)	Subverwerker	Tokio
IBM Israel Ltd.	Subverwerker	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israël

* Tot de in de bovenstaande tabel aangegeven locaties behoren de adressen van de bedrijfskantoren van de Verwerker/Subverwerker. De datacenters bevinden zich in dezelfde aangegeven landen.

De partijen of hun relevante gelieerde ondernemingen kunnen in hun desbetreffende rollen afzonderlijke standaard ongewijzigde EU Modelovereenkomsten aangaan ingevolge EC Besluit 2010/87/EU, waarbij

de optionele clausules worden verwijderd. Geschillen of aansprakelijkheden die voortvloeien uit deze overeenkomsten, ook indien ze door gelieerde ondernemingen zijn aangegaan, worden door de partijen behandeld alsof de desbetreffende geschillen of aansprakelijkheden tussen hen zijn ontstaan onder de voorwaarden van deze Overeenkomst.

Bijlage A

1. IBM SaaS-aanbiedingen

IBM biedt deze services aan als stand-alone services en aanbiedingen, of als aanvullende services en aanbiedingen. De specifiek bestelde IBM SaaS-aanbiedingen worden gespecificeerd in het Bewijs van Gebruiksrecht van Klant.

1.1 Definities van Business en Retail

De fraudeproducten van IBM Security Trusteer worden in licentie gegeven voor specifieke typen Applicaties. Een Applicatie wordt gedefinieerd als een van de volgende typen: Retail of Business. Er zijn afzonderlijke aanbiedingen verkrijgbaar voor Retail Applicaties en Business Applicaties.

- Een Retail Applicatie wordt gedefinieerd als een applicatie voor online bankieren, een mobiele applicatie of een e-commerce applicatie bedoeld voor het bedienen van consumenten. In het beleid van Klant kunnen bepaalde kleine bedrijven worden geclassificeerd als in aanmerking komend voor toegang tot retail.
- Een Business Applicatie wordt gedefinieerd als een applicatie voor online bankieren, een mobiele applicatie of een e-commerce applicatie bedoeld voor het bedienen van bedrijven, instellingen of gelijkwaardige entiteiten, of als een applicatie die niet binnen de categorie Retail valt.

1.2 IBM SaaS Basisabonnementen

Business-aanbiedingen:

- 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

Retail-aanbiedingen:

- 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

Voor elk van de Business- en Retail-aanbiedingen, met uitzondering van de IBM Security Trusteer Mobile SDK-aanbiedingen, is er voor een aanvullend bedrag een bijbehorend Premium Support-product verkrijgbaar.

1.3 Aanvullende IBM SaaS-abonnementen voor IBM Security Trusteer Rapport-aanbiedingen

Beschikbare aanvullende aanbiedingen voor 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

Beschikbare aanvullende aanbiedingen voor 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

Voor elk van de Business- en Retail-add-ons voor de IBM Security Trusteer Rapport-aanbiedingen, met uitzondering van de IBM Security Trusteer Rapport Mandatory Service-add-ons, is er voor een aanvullend bedrag een bijbehorend Premium Support-product verkrijgbaar.

Een abonnement op IBM Security Trusteer Rapport for Business of IBM Security Trusteer Rapport for Retail is een voorwaarde voor de in dit artikel beschreven bijbehorende aanvullende IBM SaaS-abonnementen.

1.4 Aanvullende IBM SaaS-abonnementen voor IBM Security Trusteer Pinpoint Malware Detection-aanbiedingen

Aanvullende aanbiedingen verkrijgbaar voor IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition of IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Aanvullende aanbiedingen verkrijgbaar voor IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition of 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

Tegen een aanvullend bedrag is er voor elk van de in dit artikel genoemde aanvullende IBM SaaS-aanbiedingen een abonnement op Premium Support verkrijgbaar.

Een abonnement op IBM Security Trusteer Pinpoint Malware Detection for Business-aanbiedingen of IBM Security Trusteer Pinpoint Malware Detection for Retail-aanbiedingen is een voorwaarde voor de in dit artikel beschreven bijbehorende aanvullende IBM SaaS-abonnementen.

1.5 Overige aanvullende IBM SaaS Abonnementen

Elk hierin niet genoemd aanvullend IBM SaaS Abonnement voor de basisabonnementen, hetzij momenteel verkrijgbaar, hetzij in ontwikkeling, wordt niet beschouwd als een update en dient afzonderlijk in licentie te worden gegeven.

1.6 Definities

Rekeninghouder – betekent de eindgebruiker van Klant, die de client-enabling software heeft geïnstalleerd, die akkoord is gegaan met de licentieovereenkomst voor eindgebruikers ("EULA") en die zich minimaal één maal heeft aangemeld bij de Retail of Business Applicatie van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen.

Clientsoftware voor Rekeninghouders – betekent de client-enabling software IBM Security Trusteer Rapport of de client-enabling software IBM Security Trusteer Mobile Browser of welke andere client-enabling software dan ook die bij bepaalde IBM SaaS-aanbiedingen wordt geleverd ten behoeve van installatie op de apparatuur van eindgebruikers.

Trusteer Splash – verwijst naar de splash die aan Klant wordt geleverd op basis van beschikbare splash templates.

Landingspagina – verwijst naar de door IBM gehoste pagina die aan Klant wordt geleverd bij de splash van Klant en de downloadbare Clientsoftware voor Rekeninghouders.

2. IBM Security Trusteer Rapport-aanbiedingen

2.1 IBM Security Trusteer Rapport for Retail en/of IBM Security Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport biedt een beschermingslaag tegen phishing en aanvallen met malware van het type Man-in-the-Browser (MitB). Met behulp van een netwerk van tientallen miljoenen eindpunten over de hele wereld verzamelt IBM Security Trusteer Rapport wereldwijd inlichtingen omtrent actieve, op organisaties gerichte aanvallen via phishing en malware. IBM Security Trusteer Rapport werkt met gedragsmatige

algoritmen gericht op het blokkeren van phishingaanvallen en het voorkómen van de installatie en exploitatie van MitB-malware.

Voor deze IBM SaaS-aanbieding geldt In Aanmerking Komende Deelnemer als maateenheid voor verschuldigde bedragen. De Business-aanbieding wordt verkocht in pakketten van 10 In Aanmerking Komende Deelnemers. De Retail-aanbieding wordt verkocht in pakketten van 100 In Aanmerking Komende Deelnemers.

Deze IBM SaaS aanbieding omvat:

a. Trusteer Management Application ("TMA"):

   De TMA wordt beschikbaar gesteld in de door de IBM Security Trusteer-cloud gehoste omgeving, via welke Klant (en een onbeperkt aantal van diens gemachtigde personeelsleden): (i) rapporten over eventgegevens en risicobeoordelingen kunnen ontvangen, (ii) het beleid inzake de rapportage van eventgegevens kunnen bekijken, configureren en instellen, en (iii) de configuratie kunnen bekijken van de client-enabling software, welke gratis aan het publiek in licentie is gegeven onder een licentieovereenkomst voor eindgebruikers ("EULA") en welke beschikbaar wordt gesteld om te worden gedownload op de desktops of apparaten (PC's/MAC's) van In Aanmerking Komende Deelnemers, ook bekend onder de naam Trusteer Rapport software suite ("Clientsoftware voor Rekeninghouders"). Klant mag de Clientsoftware voor Rekeninghouders uitsluitend verkopen met behulp van Trusteer Splash of de Rapport-API, en Klant mag de Clientsoftware voor Rekeninghouders niet gebruiken voor zijn interne bedrijfsvoering of voor gebruik door zijn werknemers (anders dan persoonlijk gebruik door werknemers).

b. Web Script:

   Voor toegang op een website ten behoeve van het verkrijgen van toegang tot, of het werken met, IBM SaaS-aanbiedingen.

c. Eventgegevens:

   Klant (en een onbeperkt aantal van diens gemachtigde personeelsleden) kan (kunnen) de TMA gebruiken voor het ontvangen van eventgegevens die door Clientsoftware voor Rekeninghouders zijn gegenereerd als gevolg van de online interacties van Rekeninghouders met de Business of Retail Applicatie van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen. Eventgegevens worden ontvangen van de Clientsoftware voor Rekeninghouders die draait op de apparatuur van In Aanmerking Komende Deelnemers die akkoord zijn gegaan met de EULA en die zich minimaal één maal hebben aangemeld bij de Retail of Business Applicatie van Klant, mits het verzamelen van Gebruikers-ID's is opgenomen in de configuratie van Klant.

d. Trusteer Splash:

   Het marketingplatform Trusteer Splash gaat na welke Clientsoftware voor Rekeninghouders geschikt is voor In Aanmerking Komende Deelnemers die zich toegang verschaffen tot de Business en/of Retail Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen. Klant kan een keuze maken uit de beschikbare Splash Templates. Er kan onder een afzonderlijke overeenkomst of werkomschrijving (statement of work) opdracht worden gegeven voor splash op maat.

Klant kan ermee akkoord gaan zijn handelsmerken, logo's of pictogrammen te verstrekken voor gebruik in samenhang met de TMA, uitsluitend ten behoeve van toepassing in de Trusteer Splash en weergave in de Clientsoftware voor Rekeninghouders of op de door IBM gehoste landingspagina's en op de website van IBM Security Trusteer. Elk gebruik van de verstrekte handelsmerken, logo's of pictogrammen van Klant vindt plaats in overeenstemming met IBM's redelijke beleid inzake publiciteit en het gebruik van handelsmerken.

Indien Klant gebruik wil maken van enig type verplichte implementatie van de Clientsoftware voor Rekeninghouders, dient Klant zich te abonneren op de SaaS-aanbieding IBM Security Trusteer Rapport Mandatory Service.

Verplichte implementatie van Clientsoftware voor Rekeninghouders omvat, maar is niet beperkt tot, elk type verplichte implementatie met behulp van enig mechanisme welk, of enige methode welke, een In Aanmerking Komende Deelnemer er rechtstreeks of indirect toe noodzaakt de Clientsoftware voor Rekeninghouders te downloaden, of enig tool of mechanisme dat, of enige methode, procedure of beleidslijn die, niet door IBM is gecreëerd of goedgekeurd en die bedoeld is voor het omzeilen van de licentievereisten van deze verplichte implementatie van de Clientsoftware voor Rekeninghouders.

2.2 Optionele aanvullende IBM SaaS-aanbiedingen voor IBM Security Trusteer Rapport for Business en/of IBM Security Trusteer Rapport for Retail

Een abonnement op IBM Security Trusteer Rapport-aanbiedingen is een voorwaarde voor een abonnement op om het even welke van de volgende aanvullende IBM SaaS-aanbiedingen. Indien de IBM SaaS is aangemerkt als "for Business", dient de aanvullende IBM SaaS-aanbieding eveneens te zijn aangemerkt als "for Business". Indien de IBM SaaS is aangemerkt als "for Retail", dient de aanvullende IBM SaaS-aanbieding eveneens te zijn aangemerkt als "for Retail". Klant ontvangt eventgegevens van de Clientsoftware voor Rekeninghouders die draait op de apparatuur van In Aanmerking Komende Deelnemers die akkoord zijn gegaan met de EULA en die zich minimaal één maal hebben aangemeld bij de Retail en/of Business Applicatie(s) van Klant, mits het verzamelen van Gebruikers-ID's is opgenomen in de configuratie van Klant.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business en/of IBM Security Trusteer Rapport Fraud Feeds for Retail

Klant (en een onbeperkt aantal van diens gemachtigde personeelsleden) kan (kunnen) de TMA gebruiken voor het ontvangen van eventgegevens met betrekking tot malware-infecties en andere kwetsbaarheden van eindpunten op de desktop van een bepaalde Rekeninghouder.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business en/of IBM Security Trusteer Rapport Phishing Protection for Retail

Klant (en een onbeperkt aantal van diens gemachtigde personeelsleden) kan (kunnen) de TMA gebruiken voor het ontvangen van meldingen van eventgegevens met betrekking tot het verstrekken van de aanmeldingsgegevens van Rekeninghouders aan een vermoedelijke phishingsite of een potentieel frauduleuze site. Legitieme online applicaties (URL's) kunnen abusievelijk worden gemarkeerd als phishingsites en de IBM SaaS kan Rekeninghouders waarschuwen dat een legitieme site een phishingsite is. In dergelijke gevallen dient Klant IBM in te lichten omtrent de desbetreffende fout en zal IBM de fout herstellen. Dit is de enige verhaalsmogelijkheid van Klant in geval van dergelijke fouten.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business en/of IBM Security Trusteer Rapport Mandatory Service for Retail

Klant mag een instance van het marketingplatform Trusteer Splash gebruiken om In Aanmerking Komende Deelnemers die zich toegang verschaffen tot de Business en/of Retail Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen, ertoe te verplichten de Clientsoftware voor Rekeninghouders te downloaden.

IBM Security Trusteer Rapport Premium Support for Business is een voorwaarde voor IBM Security Rapport Mandatory Service for Business.

IBM Security Trusteer Rapport Premium Support for Retail is een voorwaarde voor IBM Security Rapport Mandatory Service for Retail.

Klant mag de aanvullende functionaliteit van IBM Security Trusteer Rapport Mandatory Service uitsluitend implementeren indien besteld en geconfigureerd voor gebruik in combinatie met de Retail of Business Applicatie van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen.

3. IBM Security Trusteer Pinpoint-aanbiedingen

IBM Security Trusteer Pinpoint is een in de cloud werkende service die bedoeld is om een extra beschermingslaag te bieden en die zich richt op het detecteren en beperken van aanvallen via malware, phishing en accountovername. Trusteer Pinpoint kan worden geïntegreerd in de Business en/of Retail Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen.

Deze IBM SaaS aanbieding omvat:

a. TMA:

   De TMA wordt beschikbaar gesteld in de door de IBM Security Trusteer-cloud gehoste omgeving, via welke Klant (en een onbeperkt aantal van diens gemachtigde personeelsleden): (i) rapporten over eventgegevens en risicobeoordelingen kunnen ontvangen, en (ii) het beveiligingsbeleid en beleidslijnen inzake de rapportage van eventgegevens kunnen instellen.

b. Web Script en/of API's:

   Voor implementatie op een website ten behoeve van het verkrijgen van toegang tot, of het werken met, de IBM SaaS.

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

In geval van malwaredetectie door IBM Security Trusteer Pinpoint Malware Detection-aanbiedingen of detectie van accountovername door IBM Security Trusteer Pinpoint Criminal Detection-aanbiedingen dient Klant de Pinpoint Best Practices Guide te volgen. Klant mag de IBM Security Trusteer Pinpoint Malware Detection-aanbiedingen of IBM Security Trusteer Pinpoint Criminal Detection-aanbiedingen onmiddellijk na de detectie van malware of accountovername niet zodanig gebruiken dat de beleving van de In Aanmerking Komende Deelnemer op zodanige wijze wordt beïnvloed dat anderen het handelen van Klant zouden kunnen koppelen aan het gebruik van IBM Security Trusteer Pinpoint-aanbiedingen (bijv. meldingen, berichten, blokkering van apparaten, of blokkering van de toegang tot de Business en/of Retail Applicatie onmiddellijk na de detectie van malware of accountovername).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business en/of IBM Security Trusteer Pinpoint Criminal Detection for Retail

Clientloze detectie van verdachte accountovername-activiteiten van browsers die verbinding maken met een Business of Retail Applicatie, met behulp van apparaat-ID, phishingdetectie en detectie van diefstal van legitimatiegegevens met behulp van malware. IBM Security Trusteer Pinpoint Criminal Detection-aanbiedingen vormen een extra beschermingslaag, richten zich op pogingen tot accountovername en bieden Klant rechtstreeks beoordelingsscores van browsers of mobiele apparaten (via de native browser of de mobiele applicatie van Klant) die zich toegang verschaffen tot een Business of Retail Applicatie.

a. Eventgegevens:

   Klant (en een onbeperkt aantal van diens gemachtigde personeelsleden) kan (kunnen) de TMA gebruiken voor het ontvangen van eventgegevens die zijn gegenereerd als gevolg van de online interacties met de Business en/of Retail Applicatie(s) van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen, of Klant kan de eventgegevens ontvangen via een backend API-leveringsmodus.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile en/of IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

Aanbiedingen van IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) zijn ontworpen om een extra beschermingslaag te vormen en zijn erop gericht om bescherming te bieden tegen accountovername of frauduleuze activiteiten, dit middels het opsporen van onrechtmatige toegang tot accounts en het doen van aanbevelingen aan Klant. Deze IBM SaaS-aanbieding verzamelt, met behulp van de PPCD Mobile-API, informatie die afkomstig is van de Business en/of Retail Applicatie van Klant en van mobiele apparaten van In Aanmerking Komende Deelnemers. IBM Security Trusteer PPCD Mobile-aanbiedingen zijn ontworpen voor het opsporen van onderlinge verbanden tussen complexe informatie ten aanzien van mobiele apparaten van In Aanmerking Komende Deelnemers en andere gegevensbronnen, zoals real-time infecties met malware en incidenten op het gebied van phishing, welke worden geïntegreerd via de andere in deze Gebruiksvoorwaarden gespecificeerde IBM SaaS-aanbiedingen van IBM Security Trusteer.

Klant kan zich toegang verschaffen tot, en gebruikmaken van, de IBM Security Trusteer PPCD Mobile-aanbiedingen op de in de cloud gehoste omgeving van IBM Security Trusteer, en kan risicobeoordelingsgegevens ontvangen van mobiele apparaten van In Aanmerking Komende Deelnemers, welke gegevens gegenereerd zijn als gevolg van de online interacties van deze mobiele apparaten met de Business of Retail Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen. Voor het doel van deze aanbiedingen worden onder "mobiele apparaten" uitsluitend ondersteunde mobiele telefoons en tablets verstaan, geen PC's of MAC's.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition en/of IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition en/of IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition en/of IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Clientloze detectie van browsers die zijn geïnfecteerd met financiële malware van het type Man in the Browser (MitB) en die verbinding maken met een Business en/of Retail Applicatie. IBM Security Trusteer Pinpoint Malware Detection-aanbiedingen vormen een extra beschermingslaag en zijn erop gericht om organisaties in staat te stellen zich te concentreren of fraudepreventieprocessen op basis van de risico's van malware, dit door Klant te voorzien van beoordelingen en meldingen van de aanwezigheid van financiële malware van het type MitB.

a. Eventgegevens:

Klant (en een onbeperkt aantal van diens gemachtigde personeelsleden) kan (kunnen) de TMA gebruiken voor het ontvangen van eventgegevens die gegenereerd zijn als gevolg van de online interacties met de Business en/of Retail Applicatie(s) van Klant.

b. Advanced Edition:

De Advanced Editions for Business en/of for Retail bieden een aanvullende detectie- en beschermingslaag die is aangepast aan, en op maat is gemaakt voor, de structuur en stroom van de Business en/of Retail Applicaties van Klant, en die kan worden aangepast aan het specifieke dreigingslandschap waaraan Klant onderhevig is. De Advanced Editions kunnen op diverse plaatsen worden ingebouwd in de Business en/of Retail Applicaties van Klant.

De Advanced Edition wordt aan Klant aangeboden voor een aantal van minimaal 100K In Aanmerking Komende Deelnemers voor Retail of 10K In Aanmerking Komende Deelnemers voor Business, hetgeen neerkomt op 1000 pakketten van 100 In Aanmerking Komende Deelnemers voor Retail, of 1000 pakketten van 10 In Aanmerking Komende Deelnemers voor Business.

c. Standard Edition:

De Standard Edition for Business of for Retail is een snel te implementeren oplossing die de kernfunctionaliteit biedt van deze IBM SaaS-aanbieding zoals hierin beschreven.

3.2 Optionele aanvullende IBM SaaS-aanbiedingen voor IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition en/of IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition en/of IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition en/of IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Voor de IBM Security Trusteer Rapport Remediation for Retail-aanbiedingen geldt IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition of IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition als voorwaarde.

Voor IBM Security Trusteer Pinpoint Carbon Copy for Retail geldt IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition of IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition als voorwaarde. Voor IBM Security Trusteer Pinpoint Carbon Copy for Business geldt IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition of IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition als voorwaarde.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business en/of IBM Security Trusteer Pinpoint Carbon Copy for Retail

IBM Security Trusteer Pinpoint Carbon Copy-aanbiedingen zijn ontworpen voor het bieden van een extra beschermingslaag en een monitoringservice die helpt na te gaan of de legitimatiegegevens van een In Aanmerking Komende Deelnemer in gevaar zijn gekomen door Phishing-aanvallen op de Retail of Business Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail richt zich op het onderzoeken, herstellen, blokkeren en verwijderen van malware-infecties van het type man-in-the-browser (MitB) op geïnfecteerde apparaten (PC's/MAC's) van In Aanmerking Komende Deelnemers van Klant die zich op ad-hoc basis toegang verschaffen tot de Retail Applicatie van Klant, waarbij infecties met MitB-malware door IBM Security Trusteer Pinpoint Malware Detection zijn gedetecteerd op basis van eventgegevens. Klant dient een lopend abonnement te hebben op IBM Security Trusteer Pinpoint Malware Detection, feitelijk draaiend op de Retail Applicatie van Klant. Klant mag deze IBM SaaS-aanbieding uitsluitend gebruiken in samenhang met In Aanmerking Komende Deelnemers die zich toegang verschaffen tot de Retail Applicatie van Klant, en uitsluitend als tool dat zich richt op het op ad-hoc basis onderzoeken en herstellen van een bepaald geïnfecteerd apparaat (PC/MAC). IBM Security Trusteer Rapport Remediation for Retail moet feitelijk draaien op het apparaat (PC/MAC) van de desbetreffende betrokken In Aanmerking Komende Deelnemer, de desbetreffende betrokken In Aanmerking Komende Deelnemer dient akkoord te gaan met de EULA en dient zich minimaal één maal aan te melden bij de Retail Applicatie(s) van Klant, en het verzamelen van Gebruikers-ID's moet zijn opgenomen in de configuratie van Klant. Voor alle duidelijkheid: deze IBM SaaS-aanbieding geeft Klant niet het recht om de Trusteer

Splash te gebruiken en/of om de Clientsoftware voor Rekeninghouders op enige andere wijze te promoten binnen de algemene doelgroep van In Aanmerking Komende Deelnemers van Klant.

4. IBM Security Trusteer Mobile-aanbiedingen

4.1 IBM Security Trusteer Mobile Browser for Business en/of IBM Security Trusteer Mobile Browser for Retail

IBM Security Trusteer Mobile Browser is ontworpen voor het bieden van een extra beschermingslaag en richt zich op het verzorgen van veilige online toegang vanaf de mobiele apparaten van In Aanmerking Komende Deelnemers die zich toegang verschaffen tot Retail of Business Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen, alsmede op risicobeoordeling van mobiele apparaten en bescherming tegen phishing. Detectie van veilige Wi-Fi is uitsluitend beschikbaar voor Android-platforms. Voor het doel van deze IBM SaaS-aanbieding worden onder mobiele apparaten uitsluitend mobiele telefoons en tablets verstaan, geen Laptop PC's en Mac's.

Via de TMA kan Klant (en kan een onbeperkt aantal van diens gemachtigde personeelsleden) eventgegevens, analyses en statistische informatie ontvangen met betrekking tot Apparaten waarvan de In Aanmerking Komende Deelnemers: (i) de Clientsoftware voor Rekeninghouders hebben gedownload, zijnde een applicatie welke gratis aan het publiek in licentie is gegeven onder een licentieovereenkomst voor eindgebruikers ("EULA") en welke beschikbaar wordt gesteld om te worden gedownload op de mobiele apparaten van In Aanmerking Komende Deelnemers, en (ii) akkoord zijn gegaan met de EULA en zich minimaal één maal hebben aangemeld bij de Business of Retail Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen. Klant mag de Clientsoftware voor Rekeninghouders uitsluitend verkopen met behulp van de Trusteer Splash en mag de Clientsoftware voor Rekeninghouders niet gebruiken voor zijn interne bedrijfsvoering.

a. Eventgegevens:

   Klant (en een onbeperkt aantal van diens gemachtigde personeelsleden) mag (mogen) de TMA gebruiken voor het ontvangen van eventgegevens die zijn gegenereerd als gevolg van de online interacties van mobiele apparaten met de Business of Retail Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen.

b. Trusteer Splash:

   Het marketingplatform Trusteer Splash gaat na welke Clientsoftware voor Rekeninghouders geschikt is voor In Aanmerking Komende Deelnemers die zich toegang verschaffen tot de Business en/of Retail Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen. Klant kan een keuze maken uit de beschikbare splash templates ("Splash Template"). Er kan onder een afzonderlijke overeenkomst of werkomschrijving (statement of work) opdracht worden gegeven voor splash op maat.

Klant kan ermee akkoord gaan zijn handelsmerken, logo's of pictogrammen te verstrekken voor gebruik in samenhang met de TMA, uitsluitend ten behoeve van toepassing in de Trusteer Splash en weergave in de Clientsoftware voor Rekeninghouders of op de door IBM gehoste landingspagina's of op de website van IBM Security Trusteer. Elk gebruik van de verstrekte handelsmerken, logo's of pictogrammen van Klant vindt plaats in overeenstemming met IBM's redelijke beleid inzake publiciteit en het gebruik van handelsmerken.

4.2 IBM Security Trusteer Mobile SDK for Business en/of IBM Security Trusteer Mobile SDK for Retail

IBM Security Trusteer Mobile SDK-aanbiedingen zijn erop ontworpen een extra beschermingslaag te vormen. Ze richten zich op het bieden van veilige internettoegang tot de Retail en/of Business Applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen, alsmede op risicobeoordeling van apparaten en bescherming tegen pharming. Detectie van veilige Wi-Fi is uitsluitend beschikbaar voor Android-platforms.

IBM Security Trusteer Mobile SDK-aanbiedingen bestaan uit een eigen mobiele software developer's kit ("SDK"), een softwarepakket met documentatie, bibliotheken voor het programmeren van eigen software en andere bijbehorende bestanden en items, bekend als de IBM Security Trusteer mobile library, alsmede de "Runtime Component" of "Redistributable", eigen, door de IBM Security Trusteer Mobile SDK gegenereerde code die kan worden ingebed en geïntegreerd in de beschermde standalone mobiele iOS- of Android-applicaties van Klant waarvoor Klant een abonnement op IBM SaaS-aanbiedingen heeft genomen ("Door Klant Geïntegreerde Mobiele App").

IBM Security Trusteer Mobile SDK for Retail is verkrijgbaar in pakketten van 100 In Aanmerking Komende Deelnemers of pakketten van 100 Clientapparaten, en IBM Security Trusteer Mobile SDK for Business is verkrijgbaar in pakketten van 10 In Aanmerking Komende Deelnemers of pakketten van 10 Clientapparaten.

Via de TMA kan Klant (en kan een onbeperkt aantal van diens geautoriseerde personeelsleden) rapportage omtrent eventgegevens ontvangen, alsmede beoordelingen van risicotrends. Via de Door Klant Geïntegreerde Mobiele App kan Klant risicoanalyses ontvangen, alsmede informatie met betrekking tot mobiele apparatuur van de In Aanmerking Komende Deelnemers die de Door Klant Geïntegreerde Mobiele App hebben gedownload, hetgeen het voor Klant mogelijk maakt om beleid inzake fraudepreventie te formuleren, waarin risicobeperkende maatregelen ten aanzien van deze risico's worden opgelegd. Voor het doel van deze aanbieding worden onder "mobiele apparaten" uitsluitend ondersteunde mobiele telefoons en tablets verstaan, geen PC's of MAC's.

Klant mag:

a. de IBM Security Trusteer Mobile SDK intern gebruiken, uitsluitend ten behoeve van het ontwikkelen van de Door Klant Geïntegreerde Mobiele App;

b. de Redistributable als een integraal, onafscheidelijk deel inbedden (uitsluitend in de vorm van objectcode) in de Door Klant Geïntegreerde Mobiele App. Op elk deel van de Redistributable dat ingevolgde deze licentieverlening is gewijzigd of samengevoegd, zijn de bepalingen van deze Gebruiksvoorwaarden van toepassing; en

c. de Redistributable verhandelen en distribueren ten behoeve van download op mobiele apparaten van In Aanmerking Komende Deelnemers of op Clientapparaten, op voorwaarde dat:

   - Behoudens voor zover uitdrukkelijk toegestaan in deze Overeenkomst, is het Klant niet toegestaan om (1) de SDK te gebruiken, te kopiëren, te wijzigen of te distribueren; (2) de SDK omgekeerd te assembleren ("reverse assemble"), omgekeerd te compileren ("reverse compile"), of anderszins te vertalen, tenzij uitdrukkelijk rechtens toegestaan zonder dat daarvan bij contract kan worden afgeweken; (3) de SDK te verhuren of in sublicentie of lease te geven; (4) welk van de in de Redistributable opgenomen copyright- of kennisgevingsbestanden dan ook te verwijderen; (5) hetzelfde pad te gebruiken als voor de oorspronkelijke bestanden/modules van de Redistributable; en (6) zonder voorafgaande schriftelijke toestemming van IBM, diens licentiegevers en diens wederverkopers, de namen of merken van IBM, diens licentiegevers en diens wederverkopers te gebruiken in verband met de marketing van de Door Klant Geïntegreerde Mobiele App.
   - De Redistributable moet op een onafscheidelijke manier geïntegreerd blijven binnen de Door Klant Geïntegreerde Mobiele App. De Redistributable moet de vorm van objectcode behouden en moet blijven voldoen aan alle aanwijzingen, instructies en specificaties in de SDK en de bijbehorende documentatie. In de licentieovereenkomst voor de Door Klant Geïntegreerde Mobiele App moet de eindgebruiker erop worden gewezen dat de Redistributable i) niet mag worden gebruikt voor enig ander doel dan het mogelijk maken van het gebruik van de Door Klant Geïntegreerde Mobiele App, ii) niet mag worden gekopieerd (behoudens voor backupdoeleinden), iii) niet verder mag worden verspreid of overgedragen, en iv) niet omgekeerd mag worden geassembleerd ("reverse assembled"), omgekeerd worden gecompileerd ("reverse compiled") of anderszins worden vertaald, tenzij uitdrukkelijk rechtens toegestaan zonder dat daarvan bij contract kan worden afgeweken. De licentieovereenkomst van Klant dient IBM minimaal dezelfde mate van bescherming te bieden als deze Overeenkomst.
   - De SDK mag uitsluitend worden geïmplementeerd als onderdeel van interne ontwikkeling en unit testing op de gespecificeerde mobiele testapparatuur van Klant. Klant is niet gemachtigd om de SDK te gebruiken voor het verwerken van productiebelastingen, voor het simuleren van productiebelastingen of voor het testen van de schaalbaarheid van enige code, enige applicatie of enig systeem. Klant is niet gemachtigd om welk deel van de SDK dan ook te gebruiken voor enig ander doel.

Klant is verantwoordelijk voor alle technische assistentie voor de Door Klant Geïntegreerde Mobiele App en voor alle door Klant aangebrachte wijzigingen aan de Redistributables, zoals hierin toegestaan.

Klant mag de Redistributables en de IBM Security Mobile SDK uitsluitend installeren en gebruiken ter ondersteuning van het gebruik van de IBM SaaS-aanbieding door Klant.

IBM heeft tests uitgevoerd op voorbeeldapplicaties die met de bij de IBM Security Trusteer Mobile SDK geleverde mobiele tools ("Mobiele Tools") zijn gemaakt teneinde vast te stellen of deze voorbeeldapplicaties correct worden uitgevoerd op bepaalde versies van mobiele besturingssysteemplatforms van Apple (iOS), Google (Android) en anderen (gezamenlijk: "Mobiele OS Platforms"), met dien verstande echter dat Mobiele OS Platforms worden geleverd door derden, dat ze niet onder de controle van IBM vallen en dat er zonder bericht aan IBM wijzigingen in kunnen worden aangebracht. Als zodanig, en ondanks enige bepaling die het tegendeel aangeeft, garandeert IBM niet dat enige applicatie of andere invoer die met behulp van de Mobiele Tools is gemaakt, correct kan worden uitgevoerd op, samenwerkt met of compatibel is met enig Mobiel OS Platform of mobiel apparaat.

Klant verklaart nauwkeurige, geschreven documenten, uitvoer van systeemhulpprogramma's en andere systeeminformatie te creëren, te bewaren en aan IBM en haar accountants beschikbaar te stellen om tegenover IBM te kunnen aantonen dat het gebruik van de IBM Security Trusteer Mobile SDK door Klant in overeenstemming is met de bepalingen van deze Gebruiksvoorwaarden.

5. Implementatie van IBM SaaS Fraud Protection-aanbiedingen

In het basisabonnement van Klant zijn de vereiste activiteiten voor setup en initiële implementatie inbegrepen, met inbegrip van de initiële eenmalige startup, configuratie, Splash Template, testwerkzaamheden en training.

Aanvullende services kunnen voor een aanvullend bedrag worden besteld onder een afzonderlijke overeenkomst.

Bijlage B

IBM levert de volgende serviceniveau-overeenkomst (service level agreement, "SLA") inzake beschikbaarheid voor de IBM SaaS en deze is van toepassing indien gespecificeerd in het Transactiedocument van Klant:

De versie van deze SLA die actueel is op het moment dat de looptijd van het abonnement van Klant aanvangt of wordt verlengd, is van toepassing. Klant is ervan op de hoogte dat de SLA geen garantie vormt jegens Klant.

1. Definities

a. **Geautoriseerde Contactpersoon** – betekent de persoon die volgens opgave van Klant aan IBM gemachtigd is om onder deze SLA Claims in te dienen.

b. **Beschikbaarheidskrediet** – betekent de schadevergoeding die IBM zal verstrekken voor een gevalideerde Claim. Het Beschikbaarheidskrediet wordt toegekend in de vorm van een krediet of korting ten opzichte van een toekomstige factuur voor de abonnementsbedragen voor de IBM SaaS.

c. **Claim** – betekent een claim die door de Geautoriseerde Contactpersoon van Klant ingevolge deze SLA bij IBM is ingediend en waarin wordt gevorderd dat een bepaald Serviceniveau tijdens en Maand Onder Contract niet is gehaald.

d. **Maand Onder Contract** – betekent een volledige maand gedurende de looptijd van de IBM SaaS, gemeten vanaf 00:00 uur GMT op de eerste dag van de maand tot en met 23:59 uur GMT op de laatste dag van de maand.

e. **Klant** – betekent een entiteit die zich rechtstreeks bij IBM SaaS heeft geabonneerd op de Service en die voor geen van de materiële verplichtingen (waaronder begrepen betalingsverplichtingen) onder zijn overeenkomst met IBM voor de IBM SaaS in gebreke is.

f. **Downtime** – betekent een tijdsperiode gedurende welke de verwerking door de productiesystemen voor de Service is gestopt en al uw gebruikers niet in staat zijn gebruik te maken van alle aspecten van de Service waarvoor zij passende machtigingen hebben. Onder Downtime wordt niet verstaan de tijdsperiode gedurende welke de Service niet beschikbaar is als gevolg van:

- Geplande Systeem Downtime;
- Overmacht;
- Problemen met applicaties, apparatuur of gegevens van Klant of van een derde;
- Het doen en nalaten van Klant of van een derde (waaronder begrepen het verkrijgen van toegang tot de IBM SaaS door enige derde met behulp van de wachtwoorden of apparatuur van Klant);
- Verzuim om de vereiste systeemconfiguraties en ondersteunde platforms voor het benaderen van de IBM SaaS na te leven;
- Naleving door IBM van ontwerpen, specificaties of instructies die door Klant of door een derde op verzoek van Klant aan IBM zijn verstrekt.

g. **Gebeurtenis** – betekent een omstandigheid of groep omstandigheden als geheel, die ertoe leidt dat een bepaald Serviceniveau niet wordt gehaald.

h. **Overmacht** – betekent force majeure, terrorisme, arbeidsconflicten, brand, overstroming, aardbeving, rellen, oorlog, overheidsmaatregelen, -verordeningen of -restricties, virussen, denial-of-service-aanvallen en ander kwaadwillig gedrag, stroomstoringen en andere omstandigheden waaronder de IBM SaaS niet beschikbaar is als gevolg van een oorzaak die redelijkerwijs buiten de controle van IBM valt.

i. **Geplande Systeem Downtime** – betekent een geplande uitgebruikname van de IBM SaaS ten behoeve van serviceonderhoud.

j. **Serviceniveau** – betekent de hieronder aangegeven standaard volgens welke IBM het niveau van de onder deze SLA verleende service meet.

2. Beschikbaarheidskrediet

a. Om in aanmerking te komen voor het indienen van een Claim, dient Klant voor elke Gebeurtenis een ondersteuningsticket te hebben geregistreerd bij de helpdesk van IBM Customer Support voor de desbetreffende IBM SaaS, overeenkomstig de IBM-procedure voor het melden van ondersteuningsproblemen van Severity 1. Tevens dient Klant alle benodigde gedetailleerde informatie over de Gebeurtenis te verstrekken en IBM naar redelijkheid te assisteren bij het stellen van een diagnose en het oplossen van de Gebeurtenis, voor zover dat vereist is voor ondersteuningstickets van Severity 1. Dergelijke tickets moeten worden geregistreerd binnen vierentwintig (24) uur nadat voor het eerst duidelijk werd dat de Gebeurtenis negatieve gevolgen had voor het gebruik van de IBM SaaS door Klant.

b. De Geautoriseerde Contactpersoon van Klant dient de Claim van Klant voor een Beschikbaarheidskrediet in te dienen binnen drie (3) werkdagen na het einde van de Maand Onder Contract die het onderwerp van de Claim vormt.

c. De Geautoriseerde Contactpersoon van Klant dient IBM naar redelijkheid alle gegevens met betrekking tot de Claim te verstrekken, met inbegrip van, maar niet beperkt tot, gedetailleerde beschrijvingen van alle relevante Gebeurtenissen en het Serviceniveau waarvan wordt beweerd dat het niet is gehaald.

d. IBM meet de gecombineerde Downtime gedurende elke Maand Onder Contract intern zoals van toepassing op het overeenkomstige Serviceniveau dat is aangegeven in de onderstaande tabel. Het Beschikbaarheidskrediet wordt gebaseerd op de duur van de Downtime die is gemeten vanaf het tijdstip waarop Klant meldt dat hij voor het eerst met de Downtime werd geconfronteerd. Indien Klant meldt dat er gelijktijdig een Gebeurtenis van Applicatie Downtime en een Gebeurtenis van Downtime bij de Verwerking van Inkomende Gegevens optreden, behandelt IBM deze overlappende periodes van Downtime als een enkele periode van Downtime, en niet als twee afzonderlijke periodes van Downtime. Voor elke geldige Claim kent IBM het hoogste toepasselijke Beschikbaarheidskrediet toe op basis van het behaalde Serviceniveau gedurende elke Maand Onder Contract, zoals aangegeven in de onderstaande tabellen. IBM is niet aansprakelijk voor meerdere Beschikbaarheidskredieten voor dezelfde Gebeurtenis(sen) in dezelfde Maand Onder Contract.

e. Voor Gebundelde Service (afzonderlijke IBM SaaS die samen, voor een enkele gecombineerde prijs, als een pakket worden verkocht) wordt het Beschikbaarheidskrediet berekend op basis van de enkele gecombineerde maandelijkse prijs voor de Gebundelde Service en niet voor het maandelijkse abonnementsbedrag voor elke afzonderlijke IBM SaaS. Klant kan uitsluitend Claims indienen die betrekking hebben op één afzonderlijke IBM SaaS in een bundel in een willekeurige Maand Onder Contract, en IBM is niet aansprakelijk voor Beschikbaarheidskredieten met betrekking tot meer dan één IBM SaaS in een bundel in een willekeurige Maand Onder Contract.

f. Indien Klant de IBM SaaS heeft aangekocht van een geldige IBM-wederverkoper in een remarketingtransactie waarin IBM de primaire verantwoordelijkheid voor het leveren van de IBM SaaS en het naleven van de SLA-verplichtingen behoudt, wordt het Beschikbaarheidskrediet gebaseerd op de op dat moment geldende Relatie Suggested Value Price (RSVP) voor de IBM SaaS voor de Maand Onder Contract waarop een Claim betrekking heeft, onder aftrek van een korting van 50%.

g. Het totale Beschikbaarheidskrediet dat met betrekking tot enige Maand Onder Contract wordt toegekend, is in geen geval hoger dan tien procent (10%) van een twaalfde deel (1/12e) van het jaarbedrag dat Klant IBM voor de IBM SaaS heeft betaald.

h. IBM zal de geldigheid van Claims naar redelijkheid controleren aan de hand van de eigen gegevens van IBM, welke prevaleren in geval van tegenstrijdigheid met de gegevens van Klant.

i. HET BESCHIKBAARHEIDSKREDIET DAT KLANT OVEREENKOMSTIG DEZE SLA WORDT TOEGEKEND, IS DE ENIGE EN UITSLUITENDE VERHAALSMOGELIJKHEID VAN KLANT MET BETREKKING TOT WELKE VORDERING DAN OOK.

3. Serviceniveaus

Beschikbaarheid van de IBM SaaS tijdens een Maand Onder Contract

Behaald Serviceniveau (tijdens een Maand Onder Contract)	**Beschikbaarheidskrediet (% van Maandelijks Abonnementsbedrag voor Maand Onder Contract waarop een Claim betrekking heeft)**
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

"Behaald Serviceniveau", uitgedrukt als een percentage, wordt als volgt berekend: (a) het totaal aantal minuten in een Maand Onder Contract, minus (b) het totaal aantal minuten Downtime in een Maand Onder Contract, gedeeld door (c) het totaal aantal minuten in een Maand Onder Contract.

Voorbeeld: Totaal 250 minuten Downtime gedurende een Maand Onder Contract

Totaal 43.200 minuten in een Maand Onder Contract van 30 dagen - 250 minuten Downtime = 42.950 minuten _____ Totaal 43.200 minuten	= 2% Beschikbaarheidskrediet voor Behaald Serviceniveau van 99,4% tijdens de Maand onder Contract

3.1 Uitzonderingen

Deze SLA wordt uitsluitend beschikbaar gesteld aan Klanten van IBM. Deze SLA is niet van toepassing op het volgende:

- Bèta- en proef-Services.
- Niet-productieomgevingen, met inbegrip van, maar niet beperkt tot, tests, noodherstel, kwaliteitscontrole of ontwikkeling.
- Claims die zijn ingediend door gebruikers, gasten, deelnemers en toegestane genodigden van een Klant van de IBM SaaS.
- Indien Klant enige materiële verplichting onder de Gebruiksvoorwaarden niet is nagekomen, met inbegrip van, maar niet beperkt tot, niet-nakoming van enige betalingsverplichting.