American Express®
Policy operativa di sicurezza dei dati (Data Security Operating Policy) - Italia

American Express, società leader nella tutela dei propri utenti, è da tempo impegnata nella protezione delle informazioni del Cardmember, garantendone l'inviolabilità.

La compromissione dei dati produce effetti negativi su utenti, Esercenti, Fornitori di servizi e società emittenti della carta. Anche un solo incidente può compromettere seriamente la reputazione di una società e pregiudicarne la capacità di condurre affari in maniera efficace. Affrontare questa minaccia mettendo in atto procedure operative di sicurezza idonee può essere utile per accrescere la fiducia dei clienti, incrementare la redditività e migliorare la reputazione di una società.

*American Express sa di condividere questa preoccupazione con Esercenti e Fornitori di servizi (collettivamente, indicati di seguito con **voi**) e, nell'ambito delle rispettive responsabilità, chiede a questi ultimi di osservare le disposizioni in materia di sicurezza dei dati indicate nel contratto relativamente all'accettazione (nel caso degli Esercenti) o all'elaborazione (nel caso dei Fornitori di servizi) della Carta American Express® (per entrambe, rispettivamente, indicate di seguito con il termine **Contratto**), e nella presente Politica operativa di sicurezza dei dati, che può occasionalmente subire rettifiche. Tali requisiti si applicano a tutte le apparecchiature, i sistemi e le reti di Esercenti e Fornitori di servizi per mezzo dei quali sono memorizzati, elaborati o trasmessi chiavi crittografiche, Dati del Titolare di carta o Dati sensibili di autenticazione (o entrambi).*

I termini utilizzati in maiuscolo, se non vengono definiti nel presente documento, hanno il significato indicato nel glossario alla fine del presente documento.

Articolo 1 - Standard per la Protezione di Chiavi Crittografiche, Dati del Titolare di carta e Dati sensibili di autenticazione

Voi, e solidalmente le Parti contemplate, siete tenuti a:

- conservare i Dati del Titolare di carta esclusivamente per facilitare le Transazioni con Carta American Express in conformità con, e come richiesto da, il Contratto;
- osservare la versione corrente dello Standard di sicurezza dei dati di Payment Card Industry (***PCI DSS***) e dei Requisiti PCI di sicurezza per i PIN non più tardi della data di entrata in vigore di tale versione;
- usare, all'atto dell'installazione di Dispositivi per il pagamento con immissione di PIN o di Applicazioni per il pagamento (o di entrambi) nuovi o sostitutivi, solo quelli approvati da PCI.

Siete tenuti a conservare tutti gli scontrini di cassa (registrazioni di Addebito e di Credito American Express) in applicazione del Contratto secondo le presenti disposizioni in materia di sicurezza dei dati; gli scontrini andranno utilizzati esclusivamente per le finalità del Contratto e salvaguardati di conseguenza. Siete responsabili finanziariamente e in altro modo nei confronti di American Express nel garantire che le Parti contemplate agiscano in conformità con le presenti disposizioni in materia di sicurezza dei dati (fatta salva la capacità di dimostrare l'osservanza della presente *policy* ad opera delle Parti contemplate in base all'Articolo 4 riportato più avanti).

Articolo 2 - Oneri di Gestione degli Incidenti con i Dati

Eventuali Incidenti con i dati dovranno essere comunicatiad American Express immediatamente e comunque non oltre le ventiquattro (24) ore dalla loro scoperta.

Per le comunicazioni ad American Express siete pregati di contattare l'American Express Enterprise Incident Response Program (*EIRP*) al numero +1 (602) 537-3021 (il segno + indica un prefisso di chiamata internazionale diretta o "IDD"; tariffazione internazionale applicabile) oppure via e-mail all'indirizzo EIRP@aexp.com.

- Siete tenuti a nominare un responsabile come vostro contatto per la gestione del caso.
- Siete tenuti a condurre un'accurata indagine forense su ciascun Incidente con i dati. Per Incidenti con i dati che coinvolgono 10.000 o più Numeri di conto Carta

American Express (o altrimenti su richiesta di American Express), tale indagine dovrà essere condotta da un investigatore forense PCI (***PFI***).
- Siete tenuti a fornire prontamente ad American Express tutti i Numeri di Carta Compromessi e il rapporto di indagine sull'Incidente con i dati.
- Siete tenuti a collaborare con American Express per la risoluzione di tutti i problemi derivanti dall'Incidente con i dati, oltre che a consultarvi con American Express in merito alle notizie da fornire ai Cardmember American Express coinvolti nell'Incidente con i dati e fornire (e ottenere ogni deroga necessaria per tale fornitura) ad American Express ogni informazione necessaria ad accertare la vostra capacità di prevenire futuri Incidenti con i dati in maniera conforme al Contratto.

I rapporti di indagine dovranno includere esami, relazioni sulla conformità e ogni altra informazione relativa all'Incidente con i dati; dovranno identificare la causa dell'Incidente con i dati; confermare la conformità con il PCI DSS al momento dell'Incidente con i dati e accertare la vostra capacità di prevenire futuri Incidenti con i dati mediante la definizione di un piano di rimedio alle carenze emerse riguardanti il PCI DSS. Su richiesta di American Express, dovrete ottenere da un esperto qualificato in materia di valutazione della sicurezza (Qualified Security Assessor, ***QSA***) conferma dell'avvenuta risoluzione delle carenze.

A prescindere da qualsiasi obbligo di riservatezza stabilito nel Contratto, American Express ha il diritto di fornire informazioni su qualsiasi Incidente con i dati ai Cardmember American Express, alle società emittenti, agli altri partecipanti alla rete American Express e al pubblico, così come richiesto dalla legge vigente ovvero da ordinanza giudiziaria o amministrativa o da decreto, invito a comparire, petizione o altro procedimento, allo scopo di attenuare il rischio di frode o qualsiasi altro danno nella misura appropriata al mantenimento dell'operatività della rete American Express.

ARTICOLO 3 - ONERI DI RISARCIMENTO PER INCIDENTI CON I DATI

Gli oneri di risarcimento nei confronti di American Express stabiliti dal Contratto per Incidenti con i dati sono determinati, senza alcuna deroga agli altri diritti e rimedi di American Express, in base al presente Articolo 3.

American Express non vi chiederà alcun risarcimento per Incidenti con i dati (a) che coinvolgono meno di 10.000 Numeri di Carta Compromessi o (b) se:

- avrete fornito ad American Express notifica dell'Incidente con i dati conformemente all'Articolo 2 della seguente *policy*,
- al momento dell'Incidente con i dati rispettavate il PCI DSS (come stabilito dall'indagine sull'Incidente con i dati condotta dal PFI) e
- l'Incidente con i dati non è stato provocato da indebita condotta da parte vostra o delle Parti contemplate.

Il metodo di calcolo del risarcimento è indicato nell'Appendice A alla fine del presente documento.

ARTICOLO 4 - IMPORTANTE! CONVALIDA PERIODICA DEI SISTEMI IN USO

Siete tenuti all'osservanza della seguente procedura con cadenza annuale e trimestrale, secondo il PCI DSS, come descritto più avanti, allo scopo di convalidare lo stato delle apparecchiature, dei sistemi e/o delle reti (e dei relativi componenti) mediante i quali vengono memorizzati, elaborati o trasmessi i Dati del Titolare di Carta o i Dati sensibili di autenticazione.

Per completare la procedura di convalida, sono richiesti quattro passaggi:

Passaggio 1 - Iscrizione al Programma di conformità American Express ai sensi della presente *policy;*

Passaggio 2 - Determinazione del Livello e dei Requisiti di convalida;

Passaggio 3 - Determinazione della Documentazione di convalida da inviare ad American Express;

Passaggio 4 - Invio della Documentazione di convalida ad American Express.

Passaggio 1 - Iscrizione al Programma di conformità American Express ai sensi della presente *Policy*

Gli Esercenti di 1° .2° Livello e gli Esercenti di 3° Livello che American Express ha designatogli Esercenti di Livello EMV e tutti i Fornitori di servizi, secondo la definizione fornita più avanti, dovranno iscriversi al programma di conformità American Express ai sensi della presente *policy* indicando le generalità complete, l'indirizzo di posta elettronica, il numero telefonico e l'indirizzo postale di un responsabile che fungerà da proprio contatto generale per la sicurezza dei dati. Queste informazioni andranno trasmesse a Trustwave, che amministra il programma per conto di American Express, secondo uno dei metodi elencati al Passaggio 4 più avanti. Siete tenuti a comunicare a Trustwave qualsiasi variazione di queste informazioni, fornendo all'occorrenza i dati aggiornati.

American Express potrà richiedere ad alcuni Esercenti di 3° Livello di iscriversi al programma di conformità American Express ai sensi della presente *policy* inviando

loro comunicazione scritta. L'Esercente di 3° Livello designato dovrà iscriversi entro e non oltre 90 giorni dalla ricezione della comunicazione.

Passaggio 2 - Determinazione del Livello e dei Requisiti di convalida

Sono definiti cinque Livelli per gli Esercenti e due Livelli per i Fornitori di servizi. La maggior parte dei livelli è basata sul volume delle Transazioni eseguite con Carta American Express. Per gli Esercenti si prenderà in considerazioneil volume delle Transazioni così come inoltrato dalle proprie filiali e aggregato a livello di Esercente American Express. Rientrerete in uno dei Livelli specificati nelle tabelle di Esercenti e Fornitori di servizi illustrate più avanti.

Requisiti per gli Esercenti

Gli Esercenti (non i Fornitori di servizi) rientrano in una delle cinque possibili classificazioni riguardanti il livello e i requisiti di convalida. Dopo avere stabilito il livello di Esercente in base all'elenco seguente, consultate la Tabella per Esercenti per un elenco dei requisiti per la documentazione di convalida.

Esercente di 1° Livello - Almeno 2,5 milioni di Transazioni con Carta American Express per anno; oppure qualsiasi Esercente che ritiene di essere, o che American Express ritiene essere, di 1° Livello.

Esercente di 2° Livello - Da 50.000 a 2,5 milioni di Transazioni con Carta American Express per anno.

Esercente di 3° Livello (designato) - Meno di 50.000 Transazioni con Carta American Express per anno, designato da American Express per la presentazione della documentazione di convalida. Gli Esercenti designati riceveranno notifica scritta da American Express almeno 90 giorni prima della richiesta di inoltro della documentazione.

Esercente di 3° Livello (non designato) - Meno di 50.000 Transazioni con Carta American Express per anno, non designato da American Express per la presentazione della documentazione di convalida.

Esercente di Livello EMV - Esercente che non è stato coinvolto in un Incidente con i dati nei precedenti 12 mesi e che inoltre:

- Elabora almeno 50.000 Transazioni con Carta American Express per anno;
- Registra almeno il 75% di tutte le Transazioni effettuate dal Cardmember con la presentazione della Carta ;
- Tali transazioni hanno origine da Dispositivi abilitati all'uso di Chip EMV.

Tabella per Esercenti

Livello (definito sopra)	Documentazione di convalida (definita al Passaggio 3 più avanti)	Requisito
1	• Relazione annuale di valutazione della sicurezza in loco • Scansione di rete trimestrale	Obbligatorio
2	• Questionario di autovalutazione annuale • Scansione di rete trimestrale	Obbligatorio
3 Designato	• Questionario di autovalutazione annuale • Scansione di rete trimestrale	Obbligatorio
3*	• Questionario di autovalutazione annuale • Scansione di rete trimestrale	Vivamente consigliato
EMV**	• Documento di sintesi e Attestato di conformità al PCI DSS Prioritized Approach	Obbligatorio

*,Gli Esercenti di 3° Livello (diversamente dagli Esercenti di 3° Livello designati) non sono tenuti alla presentazione della Documentazione di convalida; ciò nonostante devono attenervisi, e sono ritenuti responsabili in base a tutte le altre disposizioni della presente Politica operativa di sicurezza dei dati.

**Il Livello EMV non è disponibile per gli Esercenti che hanno avuto un Incidente con i dati nei dodici (12) mesi precedenti la data di presentazione della Valutazione annuale di conformità.

Requisiti per i Fornitori di servizi

I Fornitori di servizi (non gli Esercenti) rientrano in una delle due possibili classificazioni riguardanti il livello e i requisiti di convalida. Dopo avere stabilito il livello di Fornitore di servizi in base all'elenco seguente, consultate la Tabella per Fornitori di servizi per conoscere i requisiti per la documentazione di convalida.

Fornitore di servizi di 1° Livello - Almeno 2,5 milioni di Transazioni con Carta American Express per anno; oppure qualsiasi Fornitore di servizi che ritiene di essere, o che American Express ritiene essere, di 1° Livello.

Fornitore di servizi di 2° Livello - Meno di 2,5 milioni di Transazioni con Carta American Express per anno; oppure qualsiasi Fornitore di servizi non ritenuto di 1° Livello da American Express.

Tabella per Fornitori di servizi

Livello (definito sopra)	Documentazione di convalida (definita al Passaggio 3 più avanti)	Requisito
1	• Relazione annuale di valutazione della sicurezza in loco • Scansione di rete trimestrale	Obbligatorio
2	• Questionario di autovalutazione annuale • Scansione di rete trimestrale	Obbligatorio

Passaggio 3 - Determinazione della Documentazione di convalida da inviare ad American Express

La seguente documentazione è richiesta ai diversi livelli di Esercente e Fornitore di servizi, come elencato nelle rispettive tabelle precedenti.

Valutazione annuale della sicurezza in loco - La Valutazione annuale della sicurezza in loco è una verifica dettagliata in loco delle apparecchiature, dei sistemi e delle reti (e relativi componenti) in uso mediante i quali sono memorizzati, elaborati o trasmessi i Dati del Titolare di carta o i Dati sensibili di autenticazione (o entrambi). Deve essere eseguita da:

- un QSA oppure
- da voi e certificata dal vostro amministratore delegato, direttore amministrativo e finanziario, responsabile della sicurezza delle informazioni aziendali o direttore e inviata su base annua ad American Express con l'Attestato di conformità (Attestation of Compliance, ***AOC***) pertinente.

L'AOC deve certificare la conformità a tutti i requisiti del PCI DSS e includere, se richieste, copie della relazione completa sulla conformità (Esercenti e Fornitori di servizi di 1° Livello).

Questionario di autovalutazione annuale - L'Autovalutazione annuale è un processo basato sul Questionario di autovalutazione PCI DSS (Self-Assessment Questionnaire, ***SAQ***) che vi consente di autovalutare lo stato delle apparecchiature, dei sistemi e delle reti (e relativi componenti) mediante i quali sono memorizzati, elaborati o trasmessi i Dati del Titolare di carta o i Dati sensibili di autenticazione (e entrambi). Deve essere eseguita da voi e certificata dal vostro amministratore delegato, direttore amministrativo e finanziario, responsabile della sicurezza delle informazioni aziendali o direttore. La sezione AOC del SAQ dovrà essere inviata su base annua ad American Express. La sezione AOC del SAQ deve certificare la vostra conformità a tutti i requisiti del PCI DSS e includere, se richieste, copie complete del SAQ (Esercenti di 2° e 3° Livello; Fornitori di servizi di 2° Livello).

Scansione di rete trimestrale - La Scansione di rete trimestrale è un processo che in remoto consente di accertare potenziali punti deboli e vulnerabilità della vostra rete di computer e server Web connessi a Internet. Deve essere eseguita da un Fornitore di prodotti di scansione approvato (Approved Scanning Vendor, ***ASV***). Siete tenuti a compilare e inviare su base trimestrale ad American Express l'Attestato di conformità della scansione (Attestation of Scan Compliance, ***AOSC***) allegato al Rapporto di scansione dell'ASV oppure il documento di sintesi sulle risultanze della scansione (e, se richieste, copie della scansione completa). L'AOSC o il documento di sintesi dovranno certificare che il risultato soddisfa le procedure di scansione PCI DSS, che non sono stati rilevati problemi di rischio elevato e che l'esito della scansione è stato positivo o conforme (tutti gli Esercenti ad eccezione del Livello EMV; tutti i Fornitori di servizi).

Valutazione annuale di conformità agli Obiettivi 1-4 del PCI DSS Prioritized Approach - La Valutazione annuale di conformità agli Obiettivi 1-4 del PCI DSS Prioritized Approach è una verifica delle apparecchiature, dei sistemi e delle reti (e relativi componenti) mediante i quali vengono memorizzati, elaborati o trasmessi i Dati del Titolare di carta o i Dati sensibili di autenticazione (o entrambi). Deve essere eseguita da voi e certificata dal vostro amministratore delegato, direttore amministrativo e finanziario, responsabile della sicurezza delle informazioni aziendali o direttore e inviata su base annua ad American Express con il Documento di sintesi e l'Attestato di conformità al PCI DSS Prioritized Approach (***PASAOC***). Il PASAOC deve certificare la conformità agli obiettivi 1-4 del PCI DSS Prioritized Approach e, su richiesta, includere tutti i dettagli di tale conformità (solo Esercenti di Livello EMV).

Mancata conformità al PCI DSS - Se non risultate conformi al PCI DSS, siete tenuti a compilare un AOC contenente la "Parte 4. Piano di azione per Status di non conformità" e indicare la data, non successiva ai dodici mesi dalla data dell'AOC, entro cui otterrete la conformità. L'AOC andrà trasmesso con il "Piano di azione per Status di non conformità" ad American Express, secondo uno dei metodi elencati al Passaggio 4 che segue. Dovrete fornire ad American Express aggiornamenti periodici sullo stato di attuazione della procedura di rimedio basata sul "Piano di azione per Status di non conformità" (Esercenti di 1°, 2° e 3° Livello designati; tutti i Fornitori di servizi).

American Express non applicherà nei vostri confronti le penali di mancata convalida (descritte più avanti) per la non conformità prima della data di rimedio, tuttavia sarete ritenuti responsabili nei confronti di American Express di tutti gli oneri di risarcimento per Incidente con i dati e sarete soggetti a tutte le altre disposizioni della presente politica.

Passaggio 4 - Invio della Documentazione di convalida ad American Express

Gli Esercenti di 1° Livello, 2° Livello, 3° Livello designati, gli Esercenti di Livello EMV e tutti i Fornitori di servizi sono tenuti all'invio della Documentazione di convalida indicata come "obbligatoria" nelle tabelle illustrate al Passaggio 2.

La Documentazione di convalida andrà inviata a Trustwave mediante uno dei seguenti metodi:

Portale protetto: La Documentazione di convalida potrà essere caricata mediante portale protetto di Trustwave sul sito https://login.trustwave.com.

Per istruzioni sull'utilizzo di questo portale, contattare Trustwave al numero + 800 9000 1140 o +1 (312) 267-3208 oppure via e-mail all'indirizzo AmericanExpressCompliance@trustwave.com.

Fax protetto: La Documentazione di convalida potrà essere trasmessa via fax al numero: +1 (312) 276-4019 (il segno + indica un prefisso di chiamata internazionale diretta o "IDD"; tariffazione internazionale applicabile). Includere le generalità, la denominazione sociale (DBA, Doing Business As), il nome del responsabile per la sicurezza dei dati da contattare, l'indirizzo e numero telefonico e, solo per gli Esercenti, il numero Esercente American Express di 10 cifre.

Per domande generali sul programma o sul processo descritto in precedenza, contattare Trustwave al numero + 800 9000 1140 o +1 (312) 267-3208 oppure via e-mail all'indirizzo AmericanExpressCompliance@trustwave.com

Le spese per le procedure di conformità e convalida sono a vostro carico. Con l'invio della Documentazione di convalida, dichiarate e garantite ad American Express di essere autorizzati a divulgare le informazioni ivi contenute e di fornire la Documentazione di convalida ad American Express senza violare i diritti di alcuna altra parte.

Penali di mancata convalida e Risoluzione del Contratto

American Express ha il diritto di applicare nei vostri confronti penali di mancata convalida e risolvere il Contratto se non sarete conformi a questi requisiti o se non fornirete ad American Express la Documentazione di convalida obbligatoria entro la data di scadenza pertinente. American Express provvederà a comunicarvi separatamente la data di scadenza pertinente per ciascun periodo di rendicontazione annuale e trimestrale.

Descrizione (Valuta EUR €)	Esercente o Fornitore di servizi di 1° Livello	Esercente o Fornitore di servizi di 2° Livello, Esercente di Livello EMV	Solo Esercenti di 3° Livello designati
Verrà calcolata una penale in caso di mancata ricezione della Documentazione di convalida entro la prima data di scadenza.	€19.000	€4.000	€15
Verrà calcolata un'ulteriore penale in caso di mancata ricezione della Documentazione di convalida entro 30 giorni dalla prima data di scadenza.	€26.000	€7.500	
Verrà calcolata un'ulteriore penale in caso di mancata ricezione della Documentazione di convalida entro 60 giorni dalla prima data di scadenza.	€34.000	€11.000	

Se American Express non riceverà la Documentazione di convalida obbligatoria entro 60 giorni dalla prima data di scadenza, avrà il diritto di risolvere il Contratto in conformità ai termini previsti e di applicare in maniera cumulativa nei vostri confronti le precedenti penali di mancata convalida.

ARTICOLO 5 - RISERVATEZZA

American Express adotterà ogni precauzione ragionevole per mantenere la riservatezza (e pretenderla dai propri agenti e subappaltatori, compresa Trustwave) sulle vostre relazioni sulla conformità, inclusa la Documentazione di convalida, e per non divulgare la Documentazione di convalida a terzi (ad eccezione di affiliati, agenti, rappresentanti, Fornitori di servizi e subappaltatori di American Express) per un periodo di tre anni dalla data di ricezione. Questo obbligo di riservatezza non si applica alla Documentazione di convalida che:

i. sia già nota ad American Express prima della divulgazione;
ii. sia o diventi di pubblico dominio in assenza di violazione del presente paragrafo da parte di American Express;
iii. sia debitamente consegnata a terzi da American Express senza alcun obbligo di riservatezza;

iv. sia sviluppata in maniera indipendente da American Express; oppure
v. debba essere divulgata a seguito di un'ordinanza da parte di un tribunale, un ente amministrativo o un'autorità governativa, ovvero per leggeo regolamento oppure a seguito di invito a comparire, richiesta di rivelazione, citazione o altro procedimento amministrativo o legale, oppure a seguito di qualsiasi richiesta di informazioni o indagine formale o informale da parte di un ente o autorità governativa (compresa qualsiasi autorità di contrasto della criminalità o di indagine patrimoniale).

ARTICOLO 6 - ESCLUSIONE DI RESPONSABILITÀ

AMERICAN EXPRESS DISCONOSCE QUALSIASI DICHIARAZIONE, GARANZIA E RESPONSABILITÀ IN RELAZIONE ALLA PRESENTE POLICY OPERATIVA DI SICUREZZA DEI DATI, AL PCI DSS, ALLE SPECIFICHE EMV E ALLA DESIGNAZIONE E ALL'OPERATO DI QSA, ASV O PFI (O DI ALCUNE DI QUESTE FIGURE), IN FORMA ESPLICITA, IMPLICITA, STATUTARIA O IN QUALSIASI ALTRA FORMA, INCLUSA QUALSIASI GARANZIA DI COMMERCIABILITÀ O IDONEITÀ PER UNO SCOPO SPECIFICO. LE SOCIETÀ EMITTENTI DI CARTA AMERICAN EXPRESS NON SONO TERZE PARTI BENEFICIARIE SECONDO LA PRESENTE POLICY.

Siti Web utili

Sicurezza dei dati American Express:
http://www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC:

http://www.pcisecuritystandards.org

APPENDICE A: CALCOLO DEL RISARCIMENTO

Sarete tenuti a rispondere di Incidente con i dati nel modo seguente. Nel caso di un Incidente con i dati che coinvolga solo numeri di conto Carta American Express, risarcirete prontamente American Express con il pagamento di una penale di mancata conformità per Incidente con i dati non superiore a US$ 100.000 per Incidente. Nel caso di un Incidente con i dati che coinvolga numeri di conto Carta American Express con Dati sensibili di autenticazione, risarcirete prontamente American Express per:

- Frode incrementale (definita di seguito) durante l'Intervallo temporale dell'Incidente con i dati e
- Costi di monitoraggio e sostituzione carta rispettivamente di (i) US$ 1,00 per numero di conto Carta sul 90% del totale dei Numeri di Carta Compromessi e di (ii) US $5,00 per numero di conto Carta sul 10% del totale di Numeri di Carta Compromessi, e
- Una penale di mancata conformità per Incidente con i dati non superiore a US$ 100.000 per Incidente.

American Express calcolerà la "Frode incrementale" in base alla formula seguente:

Frode incrementale = (X – Y) moltiplicato per Z, dove:

X = Totale delle perdite per frode delle società emittenti della Carta, esclusi storni di addebito e perdite da applicazioni fraudolente con Carta sui Numeri di Carta Compromessi durante l'Intervallo temporale dell'Incidente con i dati, diviso per volume totale degli addebiti registrati dalle società emittenti della Carta sui Numeri di Carta Compromessi durante l'intervallo in questione.

Y =
- Totale delle perdite per frode delle società emittenti della Carta, esclusi storni di addebito e perdite da applicazioni fraudolente con Carta American Express sui Numeri di Carta Compromessi durante l'Intervallo temporale dell'Incidente con i dati, diviso per
- Volume totale degli addebiti registrati dalle società emittenti della Carta sui Numeri di Carta non Compromessi durante l'Intervallo temporale dell'Incidente con i dati.

Z = Volume totale degli addebiti registrati dalle società emittenti della Carta sui Numeri di Carta Compromessi durante l'Intervallo temporale dell'Incidente con i dati.

American Express escluderà dal calcolo della Frode incrementale e dei Costi per monitoraggio e sostituzione carta ogni numero di conto Carta American Express coinvolto in un altro Incidente con i dati che a sua volta abbia visto coinvolti numeri di conto Carta American Express con Dati sensibili di autenticazione, purché American Express abbia ricevuto comunicazione dell'altro Incidente entro i dodici (12) mesi precedenti la Data di notifica. Tutti i calcoli eseguiti da American Express secondo questa formula sono definitivi.

Gli oneri di risarcimento dovuti dagli Esercenti per Incidenti con i dati e così definiti non saranno considerati danni incidentali, indiretti, speculativi, consequenziali, speciali, punitivi o esemplari ai sensi del Contratto, purché tali oneri non includano danni inerenti o intrinseci a perdita di profitti o ricavi, perdita di clientela o perdita di opportunità di guadagno.

APPENDICE B: GLOSSARIO

Per le finalità esclusive della presente politica si applicano le seguenti definizioni:

Carta American Express o Carta, indica

- qualsiasi carta, dispositivo di accesso al conto, apparecchio o servizio di pagamento recante nome, logo, marchio commerciale, marchio di servizio, nome commerciale o altra immagine o designazione di proprietà di American Express o di una sua affiliata e rilasciato da una società emittente oppure
- un numero di conto carta.

Attestato di conformità o AOC indica una dichiarazione dello status di conformità al PCI DSS, nella forma stabilita da Payment Card Industry Security Standards Council, LLC.

Fornitore di prodotti di scansione approvato o ASV indica una persona fisica o giuridica autorizzata da Payment Card Industry Security Standards Council, LLC alla certificazione dell'osservanza di determinati requisiti PCI DSS mediante l'esecuzione di procedure di scansione degli ambienti interfacciati a Internet alla ricerca di vulnerabilità.

Attestato di conformità della scansione o AOSC indica una dichiarazione dello status di conformità al PCI DSS basata su una scansione di rete, nella forma stabilita da Payment Card Industry Security Standards Council, LLC.

Dati del Titolare di carta ha lo stesso significato attribuitogli dal Glossario dei termini corrente per PCI DSS.

Cardmember indica una persona fisica o giuridica (i) che ha sottoscritto un accordo per l'assegnazione di un conto Carta con una società emittente o (ii) il cui nome appare sulla Carta.

Informazioni sul Cardmember indica le informazioni sui Cardmember American Express e sulle transazioni della Carta, compresi nomi, indirizzi, numeri di conto carta e numeri di identificazione carta (***CID***).

Addebito indica un pagamento o un acquisto effettuato con una Carta.

Chip indica un microchip integrato inserito in una Carta contenente le informazioni sul Cardmember e sul conto.

Carta con chip indica una carta contenente un Chip che può richiedere un PIN come strumento di verifica dell'identità del Cardmember o delle informazioni sul conto contenute nel Chip, ovvero di entrambe (a volte indicata nella nostra documentazione come "smart card", "Carta EMV", "ICC" o "carta con circuito integrato").

Dispositivo abilitato all'uso di Chip indica un apparecchio POS con approvazione/certificazione EMVco (www.emvco.com) valida e aggiornata in grado di elaborare Transazioni con Carta con Chip conformi a AEIPS.

Numero di Carta Compromesso indica un numero di conto Carta American Express correlato a un Incidente con i dati.

Parti contemplate indica tutti i dipendenti, agenti, rappresentanti, subappaltatori, Responsabili dell'elaborazione, Fornitori di servizi, fornitori di apparecchi o sistemi POS o di soluzioni per l'elaborazione dei pagamenti afferenti a Esercenti e Fornitori di servizi, e ogni altra parte a cui può essere fornito accesso alle Informazioni sul Cardmember conformemente al Contratto.

Credito indica l'importo dell'Addebito rimborsato ai Cardmember per acquisti o pagamenti effettuati con la Carta.

Incidente con i dati indica un incidente che implica la compromissione delle chiavi crittografiche American Express, o di almeno un numero di conto Carta American Express in cui avviene:

- l'accesso non autorizzato o l'uso dei Dati del Titolare di carta o dei Dati sensibili di autenticazione (o di entrambi) che sono memorizzati, elaborati o trasmessi con le apparecchiature, i sistemi e/o le reti (o i relativi componenti) in dotazione presso gli Esercenti e i Fornitori di servizi;
- l'uso dei Dati del Titolare di carta o dei Dati sensibili di autenticazione (o di entrambi) diverso da quello stabilito in conformità con il Contratto; e/o
- la perdita, il furto o l'appropriazione indebita presunta o acclarata di qualsiasi mezzo, materiale, registro o informazione contenente Dati del Titolare di carta o Dati sensibili di autenticazione.

Intervallo temporale dell'Incidente con i dati indica l'intervallo di tempo che ha inizio 365 giorni prima della Data di notifica e termina 30 giorni dopo tale Data.

Specifiche EMV indica le specifiche pubblicate da EMVCo, LLC, e disponibili sul sito http://www.emvco.com.

Transazione EMV indica una transazione con carta con circuito integrato (a volte indicata come "Carta IC", "carta con chip", "smart card", "Carta EMV" o "ICC") condotta su un terminale POS (point of sale) in grado di accettare carte IC e dotato di approvazione di tipo EMV valida e aggiornata. Le approvazioni di tipo EMV sono disponibili sul sito http://www.emvco.com.

Chiave crittografica ("chiave crittografica American Express") **indica** tutte le chiavi usate nell'elaborazione, creazione, caricamento e/o protezione dei Dati sul conto. Sono incluse, a titolo esemplificativo ma non esaustivo:

- Le Key Encrypting Key: Zone Master Key (ZMK) e Zone Pin Key (ZPK)
- Le Master Key usate nei dispositivi a crittografia protetta: Local Master Key (LMK)
- Le Card Security Code Key (CSCK)
- Le PIN Key: Base Derivation Key (BDK), PIN Encryption Key (PEK) e ZPK

Esercente di 1° Livello - Almeno 2,5 milioni di Transazioni con Carta American Express per anno; oppure qualsiasi Esercente che ritiene di essere, o che American Express ritiene essere, di 1° Livello.

Esercente di 2° Livello - Da 50.000 a 2,5 milioni di Transazioni con Carta American Express per anno.

Esercente di 3° Livello - Meno di 50.000 Transazioni con Carta American Express per anno, non designato da American Express.

Esercente di 3° Livello (designato) indica gli Esercenti che hanno ricevuto da American Express notifica dell'obbligo di partecipazione al programma di Conformità PCI American Express e di segnalazione del proprio status di conformità.

Fornitore di servizi di 1° Livello - Almeno 2,5 milioni di Transazioni con Carta American Express per anno; oppure qualsiasi Fornitore di servizi che ritiene di essere, o che American Express ritiene essere, di 1° Livello.

Fornitore di servizi di 2° Livello - Meno di 2,5 milioni di Transazioni con Carta American Express per anno; oppure qualsiasi Fornitore di servizi non ritenuto di 1° Livello da American Express.

Esercente di Livello EMV - Esercente che non è stato coinvolto in un Incidente con i dati nei precedenti 12 mesi e che inoltre:

- Elabora almeno 50.000 Transazioni con Carta American Express per anno;
- Registra almeno il 75% del totale delle Transazioni eseguite con la presentazione della Carta e originate su Sistemi POS conformi alle Specifiche EMV di American Express.

Obiettivi 1-4 indica le priorità assegnate ai requisiti PCI DSS dal protocollo PCI Prioritized Approach, disponibile sul sito https://www.pcisecuritystandards.org.

Data di notifica indica la data, stabilita da American Express, in cui le società emittenti riceveranno notifica dell'Incidente con i dati.

Applicazione per il pagamento ha lo stesso significato attribuitogli dal Glossario dei termini corrente per Payment Card Industry Payment Application Data Security Standard, disponibile sul sito https://www.pcisecuritystandards.org.

Approvato da PCI indica che un Dispositivo per il pagamento con immissione di PIN o un'Applicazione per il pagamento (o entrambi) appaiono, al momento della loro commercializzazione, nell'elenco delle società e dei fornitori approvati gestito da PCI Security Standards Council, LLC, disponibile sul sito https://www.pcisecuritystandards.org.

PCI DSS indica Payment Card Industry Data Security Standard, lo standard di sicurezza dei dati di PCI, disponibile sul sito https://www.pcisecuritystandards.org.

PCI DSS Prioritized Approach ha lo stesso significato attribuitogli dal Glossario dei termini corrente per PCI DSS.

Documento di sintesi e Attestato di conformità al PCI DSS Prioritized Approach o PASAOC indica una dichiarazione dello status di conformità al protocollo PCI DSS Prioritized Approach, nella forma stabilita da Payment Card Industry Security Standards Council, LLC.

Investigatore forense PCI o PFI indica una persona fisica o giuridica autorizzata da Payment Card Industry Security Standards Council, LLC alla conduzione di indagini forensi su

una violazione o una compromissione dei dati della carta di pagamento.

Requisiti di sicurezza PCI per i PIN indica i requisiti di sicurezza per i PIN di Payment Card Industry, disponibili sul sito https://www.pcisecuritystandards.org.

Dispositivo per il pagamento con immissione di PIN ha lo stesso significato attribuitogli dal Glossario dei termini corrente per i requisiti di sicurezza modulare PTS (PIN Transaction Security) POI (Point of Interaction) di Payment Card Industry, disponibile sul sito https://www.pcisecuritystandards.org.

Sistema POS (Point of Sale) indica un sistema o un'apparecchiatura per l'elaborazione di informazioni, costituito da terminale, PC, registratore di cassa elettronico, lettore contactless, o da un modulo o un processo di pagamento, utilizzato da un Esercente per ottenere autorizzazioni e/o per raccogliere dati sulle Transazioni.

Responsabile dell'elaborazione indica un fornitore di servizi agli Esercenti che facilita l'autorizzazione e l'elaborazione degli inoltri alla rete American Express.

Esperto qualificato in materia di valutazione della sicurezza o QSA indica una persona fisica o giuridica autorizzata da Payment Card Industry Security Standards Council, LLC alla certificazione dell'osservanza del PCI DSS.

Questionario di autovalutazione o SAQ indica uno strumento di autovalutazione creato da Payment Card Industry Security Standards Council, LLC allo scopo di valutare e attestare la conformità al PCI DSS.

Dati sensibili di autenticazione ha lo stesso significato attribuitogli dal Glossario dei termini corrente per PCI DSS.

Fornitori di servizi indica responsabili delle elaborazioni autorizzati, responsabili delle elaborazioni di terzi, fornitori di gateway e qualsiasi altro fornitore per Esercenti di apparecchiature, software o sistemi POS, o di altre soluzioni o servizi per l'elaborazione dei pagamenti.

Transazione indica una operazione di Addebito o Credito completata mediante l'uso di una Carta.

Documentazione di convalida indica l'AOC presentato riguardo a una Valutazione annuale della sicurezza in loco o SAQ, l'AOSC e i documenti di sintesi delle risultanze presentati riguardo alle Scansioni di rete trimestrali oppure l'Attestato EMV annuale.