AMERICAN EXPRESS

Procedura operativa di sicurezza dei dati

AMERICAN EXPRESS

Riepilogo delle modifiche DSOP

Icone

Gli aggiornamenti importanti sono elencati nella Tabella di riepilogo delle modifiche e indicati inoltre nella *DSOP* con una barra di modifica. Una barra di modifica è una linea verticale, di solito nel margine sinistro, che identifica il testo aggiunto o modificato. Solo le modifiche sostanziali alla *DSOP* con potenziali ripercussioni sulle procedure operative dell'Esercizio sono indicate con una barra di modifica, come illustrato sul margine sinistro.

Il testo eliminato viene evidenziato con un'icona a forma di cestino posta a margine di ogni eliminazione significativa di testo, compresi gli articoli, le tabelle, i paragrafi, le note e i punti elenco. Il testo eliminato viene citato in questo Riepilogo delle modifiche utilizzando la numerazione degli articoli della precedente edizione per evitare confusione.

Le strisce blu che delimitano i paragrafi indicano le informazioni specifiche dell'area geografica.

Tabella di riepilogo delle modifiche

Gli aggiornamenti importanti sono elencati nella seguente tabella e indicati inoltre nella *DSOP* con una barra di modifica.

Articolo/Comma	Descrizione della modifica
Non ci sono modifiche per questa versione.	

Articolo 1 Introduzione alla DSOP e agli Standard per la Protezione

American Express, società leader nella tutela dei propri utenti, è da tempo impegnata nella protezione dei Dati dei Titolari della Carta e dei Dati sensibili di autenticazione, garantendone l'inviolabilità.

La compromissione dei Dati produce effetti negativi su consumatori, Esercizi, 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 dell'azienda.

American Express sa di condividere questa preoccupazione con Esercizi e Fornitori di servizi (collettivamente, indicati di seguito con il termine **voi**) e, nell'ambito delle loro rispettive responsabilità, chiede a questi ultimi di osservare le disposizioni in materia di sicurezza dei Dati indicate nell'Accordo relativamente all'accettazione (nel caso degli Esercizi) o all'emissione (nel caso dei Fornitori di servizi) della Carta American Express® (entrambe tali disposizioni indicate rispettivamente con il termine **Accordo**) e la presente Procedura operativa di sicurezza dei dati (DSOP), che può occasionalmente subire rettifiche. Tali requisiti si applicano a tutte le apparecchiature, i sistemi e le reti (e i loro rispettivi componenti) per mezzo dei quali sono conservati, elaborati o trasmessi chiavi crittografiche, dati del Titolare di Carta o Dati sensibili di autenticazione (o una combinazione di questi).

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

La Procedura operativa di sicurezza dei dati (DSOP) è un insieme di requisiti di politica completi concepiti per proteggere i Dati del conto ogni volta che tali Dati vengono archiviati, elaborati o trasmessi.

American Express richiede che tutti gli Esercizi e i Fornitori di servizi siano conformi al Payment Card Industry Data Security Standard (PCI DSS). Come parte di tale requisito, voi, e solidalmente le Parti contemplate, siete tenuti a:

- conservare i Dati del Titolare della Carta esclusivamente per facilitare le transazioni con Carta American Express in conformità con, e come richiesto dall'Accordo;
- osservare la versione corrente dello Standard di sicurezza dei dati di Payment Card Industry (PCI DSS) e altri requisiti PCI Security Standards Council (PCI-SSC) applicabili per le vostre operazioni di elaborazione, conservazione e trasmissione di chiavi di crittografia, dei Dati del Titolare della Carta o dei Dati sensibili di autenticazione entro la data di entrata in vigore del requisito applicabile;
- assicurarsi che vengano utilizzati prodotti approvati PCI quando si implementa o si sostituisce la tecnologia per conservare, elaborare o trasmettere i dati.

Voi siete tenuti a proteggere tutta la Documentazione di Addebito e Credito American Express, conservata in conformità con quanto stabilito dall'Accordo secondo le presenti disposizioni in materia di sicurezza dei Dati; tale documentazione deve essere utilizzata esclusivamente per le finalità dell'Accordo e salvaguardata di conseguenza. Siete responsabili finanziariamente e per altri aspetti 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 procedura ad opera delle Parti contemplate secondo l'Articolo 2, "Programma di conformità PCI DSS (Importante Convalida periodica dei Sistemi in uso)", a meno che sia presente diversa disposizione in tale articolo). I dettagli sugli standard PCI e su come ottemperare ai suoi requisiti sono disponibili all'indirizzo www.pcisecuritystandards.org.

Articolo 2 Programma di conformità PCI DSS (Importante Convalida periodica dei Sistemi in uso)

Siete tenuti all'osservanza della seguente procedura con cadenza annuale e ogni 90 giorni, 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) vostre e dei vostri Affiliati mediante i quali vengono memorizzati, elaborati o trasmessi i Dati del Titolare della Carta o i Dati sensibili di autenticazione.

Per completare la procedura di convalida le fasi da seguire sono quattro:

- Azione 1: Partecipazione al Programma di conformità PCI American Express ai sensi della presente procedura.
- Azione 2: Riconoscimento del proprio Livello di Esercizio/Fornitore di servizi e dei Requisiti della Documentazione di convalida.
- Azione 3: Compilazione della Documentazione di convalida da inviare ad American Express.
- Azione 4: Invio della Documentazione di convalida ad American Express nei tempi stabiliti.

Azione 1: Partecipazione al Programma di conformità American Express ai sensi della presente Procedura

Gli Esercizi di Livello 1° e 2° e tutti i Fornitori di servizi, secondo la definizione fornita a seguire, dovranno partecipare al Programma ai sensi della presente procedura. American Express può richiedere, a sua esclusiva discrezione, ad alcuni Esercizi di 3° e 4° Livello di partecipare al Programma ai sensi della presente procedura.

Gli Esercizi e i Fornitori di servizi cui è richiesto di partecipare al Programma sono tenuti a registrarsi al Portale fornito dall'Amministratore del Programma scelto da American Express entro i tempi previsti.

- È necessario accettare tutti i Termini e Condizioni ragionevoli associati all'uso del Portale.
- È necessario affidare e fornire informazioni accurate ad almeno una persona di contatto relativamente alla sicurezza dei Dati contenuti nel Portale. Le informazioni richieste includono:
  - nome completo
  - indirizzo e-mail
  - numero telefonico
  - indirizzo postale
- È necessario fornire informazioni di contatto nuove o aggiornate alla persona incaricata della sicurezza dei Dati contenuti nel Portale qualora tali informazioni subiscano variazioni.
- È necessario assicurarsi che i propri sistemi siano aggiornati per permettere le comunicazioni di servizio dal dominio designato del Portale.

Se l'utente non fornisce o non mantiene informazioni di contatto aggiornate per comunicazioni sulla sicurezza dei Dati o non abilita le comunicazioni via e-mail, ciò non influirà sul nostro diritto di richiedere delle penali.

Azione 2: Riconoscimento del proprio Livello di Esercizio/Fornitore di servizi e dei requisiti della Documentazione di convalida

I Livelli applicabili agli Esercizi sono quattro, mentre quelli applicabili ai Fornitori di servizi sono due, in base al volume delle transazioni eseguite con Carta American Express.

- Per gli Esercizi, questo corrisponde al volume trasmesso dai loro Punti vendita che raggiungono il massimo livello di conto Esercizio American Express.*
- Per i Fornitori di servizi, questo corrisponde al volume trasmesso dal Fornitore di Servizi e dai Fornitori di Servizi che operano per conto di altre Entità.

Per determinare il Livello di Esercizio e i Requisiti di convalida, le transazioni BIP (Buyer Initiated Payment) sono escluse dal volume delle transazioni effettuate con Carta American Express. L'Esercizio ricadrà in uno dei Livelli di Esercizio specificati nella Tabella A-1: Livelli degli Esercizi e dei Fornitori di servizi.

* Nel caso degli Affillianti, è incluso il volume dei Punti vendita degli Affilliati. Gli Affilianti che danno mandato ai propri Affiliati di usare uno specifico terminale POS (Point of Sale) o Fornitore di servizi dovranno anche fornire la Documentazione di convalida relativa agli Affiliati coinvolti.

Tabella A-1: Livelli degli Esercizi e dei Fornitori di servizi

Livello del Fornitore dell'Esercizio	Transazioni annuali American Express
Esercizio di 1° Livello	Almeno 2,5 milioni di transazioni (o più) con Carta American Express all'anno; oppure qualsiasi Esercizio a cui American Express, a sua esclusiva discrezione, assegni il 1° Livello.
Esercizio di 2° Livello	Da 50.000 a meno di 2,5 milioni di transazioni con Carta American Express all'anno.
Esercizio di 3° Livello	Da 10.000 a meno di 50.000 transazioni con Carta American Express all'anno.
Esercizio di 4° Livello	Meno di 10.000 transazioni con Carta American Express all'anno.
Livello del Fornitore di servizi	**Transazioni annuali American Express**
Fornitore di servizi di 1° Livello	Almeno 2,5 milioni di transazioni o più con Carta American Express per anno; oppure qualsiasi Fornitore di servizi che American Express designi come 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.

Requisiti relativi alla Documentazione di convalida dell'Esercizio

Gli Esercizi (non Fornitori di servizi) rientrano in una tra quattro possibili classificazioni riguardanti il Livello di Esercizio. Dopo aver determinato il livello dell-Esercizio sulla base della Tabella A-1: Livelli degli Esercizi e dei Fornitori di servizi (sopra), vedere la Tabella A-2: Documentazione di convalida dell'Esercizio per determinare i requisiti relativi alla documentazione di convalida.

Tabella A-2: Documentazione di convalida dell'Esercizio

Livello dell'Esercizio/ transazioni annuali con Carta American Express	Relazione sulla conformità Attestato di conformità (ROC AOC)	Questionario di autovalutazione Attestato di conformità (SAQ AOC) E Scansione esterna trimestrale della vulnerabilità di rete (Scansione)	Attestato STEP (Security Technology Enhancement Program) per gli Esercizi qualificati a partecipare al programma
1° livello/ 2,5 milioni o più	Obbligatorio	Non applicabile	Facoltativo con l'approvazione da parte di American Express (sostituisce il ROC)
2° livello/ da 50,000 a meno di 2,5 milioni	Facoltativo	SAQ AOC obbligatorio (a meno che si presenti un ROC AOC); scansione obbligatoria per determinati tipi di SAQ	Facoltativo con l'approvazione da parte di American Express* (sostituisce il SAQ e la scansione di rete o il ROC)
3°** livello/ Da 10.000 a meno di 50.000	Facoltativo	SAQ AOC facoltativo (obbligatorio se richiesto da American Express); scansione obbligatoria con determinati tipi di SAQ	Facoltativo con l'approvazione da parte di American Express* (sostituisce il SAQ e la scansione di rete o il ROC)
4°** livello/ Meno di 10.000	Facoltativo	SAQ AOC facoltativo (obbligatorio se richiesto da American Express); scansione obbligatoria con determinati tipi di SAQ	Facoltativo con l'approvazione da parte di American Express* (sostituisce il SAQ e la scansione di rete o il ROC)

* **Nota:** il team PCI di American Express esaminerà la richiesta e l'eleggibilità e confermerà se siete qualificati per il Programma STEP. Rivolgersi al proprio Client Manager e/o all'inidirizzo AXPPCIComplianceProgram@aexp.com per verificare la propria idoneità.

**A scanso di equivoci, gli Esercizi di 3° e 4° Livello non sono tenuti alla presentazione della Documentazione di convalida, a meno che non sia richiesta a discrezione di American Express; ciò nonostante devono attenervisi, e sono ritenuti responsabili per tutte le altre disposizioni della presente Procedura operativa di sicurezza dei dati.

American Express si riserva il diritto di verificare la completezza, l'accuratezza e l'adeguatezza della Documentazione di convalida PCI. Per una valutazione meglio documentata di tale verifica, American Express potrebbe richiedere all'Esercizio di fornire ulteriori documenti a supporto. Inoltre, American Express ha il diritto di richiedere all'Esercizio di coinvolgere un Esperto qualificato in materia di valutazione della sicurezza (QSA) o Investigatore forense PCI (PFI) approvato dal PCI Security Standards Council.

Requisiti della Documentazione di convalida del Fornitore di servizi

I Fornitori di servizi (non Esercizi) hanno due possibili Livelli di classificazione. Dopo aver determinato il Livello del Fornitore di servizi sulla base della Tabella A-1: Livelli degli Esercizi e dei Fornitori di servizi (sopra), vedere la Tabella A-3: Documentazione di convalida del Fornitore di servizi per determinare i requisiti relativi alla documentazione di convalida.

I Fornitori di servizi non possono essere ammessi al programma STEP.

Tabella A-3: Documentazione di convalida del Fornitore di servizi

Livello	Documentazione di convalida	Requisito
1	Relazione annuale sulla conformità Attestato di conformità (ROC AOC)	Obbligatorio
2	SAQ D annuale (Fornitore di servizi) e Scansione di rete trimestrale o Relazione annuale sulla conformità Attestato di conformità (ROC AOC), se preferibile	Obbligatorio

È preferibile che anche i Fornitori di servizi si conformino alle disposizioni della Convalida supplementare delle Entità designate PCI.

Programma Security Technology Enhancement (STEP)

A discrezione di American Express, gli Esercizi che sono conformi al PCI DSS possono essere ammessi al programma di ampliamento della tecnologia di sicurezza o STEP di American Express se mettono in atto determinate misure aggiuntive di sicurezza tecnologiche nel proprio ambiente di elaborazione delle Carte. Il Programma STEP si applica solo se l'Esercizio non è incorso in alcun Incidente con i dati nei precedenti 12 mesi e se il 75% di tutte le transazioni con Carta dell'Esercizio viene effettuato mediante la combinazione delle seguenti opzioni aggiuntive di sicurezza:

- **EMV, EMV Contactless o Portafoglio digitale** – su un Dispositivo attivo abilitato all'uso di Chip dotato di approvazione/certificazione EMVCo (www.emvco.com) valida e aggiornata in grado di elaborare transazioni con Carta con Chip conformi a AEIPS. (Gli Esercizi statunitensi devono includere la funzionalità Contactless)
- **Crittografia Point-to-Point (P2PE)** – in comunicazione con il processore dell'Esercizio attraverso un sistema di crittografia Point-to-Point approvato dal PCI SSC o da un QSA
- **Con Token** - la soluzione di tokenizzazione implementata deve:
  - soddisfare le specifiche EMVCo,
  - essere tenuta al sicuro, elaborata, memorizzata, trasmessa e interamente gestita da un fornitore di servizi terzo conforme PCI, e
  - il Token non può essere annullato per rivelare Numeri di conto principale (PAN) all'Esercizio.

Gli Esercizi che possono essere ammessi al programma STEP hanno requisiti ridotti riguardo alla Documentazione di convalida PCI, come descritto ulteriormente più avanti nella Azione 3: "Compilazione della Documentazione di convalida da inviare ad American Express" come sotto riportato.

Azione 3: Compilazione della Documentazione di convalida da inviare ad American Express

I seguenti documenti sono richiesti per i diversi livelli dell'Esercizio e del Fornitore di servizi sulla base della Tabella A-2: Documentazione di convalida dell'Esercizio e della Tabella A-3: Documentazione di convalida del Fornitore di servizi riportata sopra.

L'Esercizio dovrà fornire l'Attestato di Conformità (AOC) per il tipo di valutazione applicabile. L'AOC è una dichiarazione dello stato di conformità e, come tale, deve portare la firma e la data apposte dal livello dirigenziale appropriato all'interno dell'organizzazione dell'Esercizio.

Oltre all'AOC, American Express potrebbe richiedere all'Esercizio di fornire una copia della valutazione completa, e, a sua sola discrezione, ulteriori documenti a supporto che dimostrino la conformità ai requisiti PCI DSS. Questa Documentazione di convalida è raccolta a spese dell'Esercizio.

Relazione sulla conformità Attestato di conformità (ROC AOC) - (Requisito annuale) – La Relazione sulla conformità documenta i risultati di un esame dettagliato in loco delle apparecchiature, sistemi e reti (e loro componenti) dell'Esercizio, mediante i quali sono memorizzati, elaborati o trasmessi i Dati del Titolare di Carta o i Dati sensibili di autenticazione (o entrambi). Esistono due versioni: una per gli Esercizi e un'altra per i Fornitori di servizi. La Relazione sulla conformità deve essere redatta:

- da un QSA, oppure
- da un Valutatore interno della sicurezza (ISA) e certificata dal vostro amministratore delegato, direttore amministrativo e finanziario, responsabile della sicurezza delle informazioni aziendali o direttore.

Il ROC AOC deve portare firma e data apposte da un QSA o ISA e dal livello dirigenziale appropriato all'interno dell'organizzazione dell'Esercizio ed essere inviata ad American Express almeno una volta all'anno.

Questionario di autovalutazione Attestato di conformità (SAQ AOC) - (Requisito annuale) – I Questionari di autovalutazione consentono l'autovalutazione dello stato delle apparecchiature, dei sistemi e delle reti (e relativi componenti) dell'Esercizio, mediante i quali sono memorizzati, elaborati o trasmessi i Dati del Titolare della Carta o i Dati sensibili di autenticazione (o entrambi). Esistono diverse versioni del SAQ. Ne selezionerete una o più in base al vostro ambiente di dati dei Titolari della Carta.

Il SAQ può essere compilato solo da personale interno all'Azienda qualificato a rispondere accuratamente e pienamente alle domande oppure l'Esercizio può rivolgersi a un QSA per ottenere assistenza. Il SAQ AOC deve portare firma e data apposte dal livello dirigenziale appropriato all'interno dell'organizzazione dell'Esercizio ed essere inviata ad American Express almeno una volta all'anno.

Riepilogo scansione vulnerabilità di rete esterna effettuata dal fornitore di scansioni autorizzato (Scansione ASV) - (Requisito ogni 90 giorni) – Una scansione della vulnerabilità eseguita al di fuori della rete è un test remoto eseguito per aiutare ad identificare potenziali punti deboli, vulnerabilità e errori di configurazione di componenti di interfaccia Internet dell'Ambiente Dati del Titolare di Carta dell'Esercizio (ad es. siti web, applicazioni, server web, server di posta, domini pubblici o host).

La Scansione ASV deve essere eseguita da un Fornitore Autorizzato per la Scansione (ASV).

Se richiesto dal SAQ, occorrerà trasmettere ad American Express almeno una volta ogni 90 giorni la Relazione ASV Scan di Attestato di conformità della Scansione (AOSC) o un riepilogo generale che includa il conto degli obiettivi scansionati, una certificazione che indichi che i risultati soddisfano le procedure di scansione PCI DSS e lo status di conformità raggiunto dall'ASV.

ROC AOC o STEP non saranno necessari per fornire un riepilogo generale della Scansione AOSC o ASV, se non specificamente richiesto. A scanso di qualsiasi equivoco, le Scansioni sono obbligatorie se richieste dal SAQ applicabile.

Documentazione di convalida dell'Attestato annuale del Programma STEP – (Requisito annuale) – Lo STEP è a disposizione solo degli Esercizi che soddisfano i requisiti elencati nella Azione 2: "Riconoscimento del proprio Livello di Esercizio/Fornitore di servizi e dei requisiti della Documentazione di convalida" sopra. Se la vostra azienda rientra in questa qualifica, occorrerà completare e presentare ad American Express il modulo

dell'Attestato STEP una volta all'anno. Il modulo di Attestato annuale STEP è disponibile per il download dal Portale. Potete anche rivolgervi al vostro Gestore clienti o scrivere ad American Express all'indirizzo AXPPCIComplianceProgram@aexp.com.

Non conformità PCI DSS - (Requisito annuale, ogni 90 giorni e/o ad hoc) – Qualora l'Esercizio non fosse conforme ai requisiti PCI DSS, sarà tenuto a presentare un Riepilogo Strumenti di Approccio prioritario (PAT) PCI (scaricabile tramite il sito web del PCI Security Standards Council).

Il riepilogo PAT deve indicare una data entro cui porre rimedio al problema, che non dovrà superare, al fine di ottenere la conformità, i dodici (12) mesi dalla data di compilazione della documentazione. Dovrete fornire ad American Express aggiornamenti periodici sullo stato di attuazione della procedura di correzione del vostro Status di non conformità (Esercizi di 1°, 2°, 3° e 4° Livello; tutti i Fornitori di servizi). Le azioni correttive necessarie per ottenere la conformità al PCI DSS devono essere portate a termine a vostre spese.

American Express non imporrà penali di mancata convalida prima della data di correzione. Ai sensi della Tabella A-4: Penali di mancata convalida, l'Esercizio rimane responsabile nei confronti di American Express per tutti gli obblighi di risarcimento per un Incidente con i dati ed è soggetto a tutte le altre disposizioni della presente procedura.

American Express, a sua esclusiva discrezione, si riserva il diritto di imporre penali di mancata convalida se:

- un Modello di approccio prioritario PCI non è stato presentato in conformità con i requisiti indicati in questo articolo;
- le azioni di correzione delineate nel Modello di approccio prioritario PCI per lo stato di non conformità non sono state eseguite;
- uno qualsiasi dei requisiti del Modello di approccio prioritario PCI per lo stato di non conformità non è stato soddisfatto, oppure
- la documentazione di conformità obbligatoria non è stata fornita ad American Express entro la scadenza prevista o richiesta.

Gli Esercizi/Fornitori di servizi che non rispettano i requisiti descritti nell'Azione 2: Riconoscimento del proprio Livello di Esercizio/Fornitore di servizi e dei requisiti della Documentazione di convalida, possono essere soggetti a penali come stabilito nell'Azione 4: Invio della Documentazione di convalida ad American Express.

A scanso di qualsiasi equivoco, gli Esercizi non conformi al PCI DSS non saranno qualificati a partecipare al Programma STEP.

Azione 4: Invio della Documentazione di convalida ad American Express

Tutti gli Esercizi e i Fornitori di servizi cui è richiesto di partecipare al Programma sono tenuti a presentare la Documentazione di convalida indicata come "obbligatoria" nelle tabelle illustrate nell'Azione 2: "Riconoscimento del proprio Livello di Esercizio/Fornitore di servizi e dei requisiti della Documentazione di convalida" ad American Express entro le date di scadenza applicabili.

Dovrete presentare la Documentazione di convalida ad American Express usando il Portale fornito dall'Amministratore del Programma scelto da American Express. Presentando la Documentazione di convalida, l'Esercizio dichiara e garantisce ad American Express che quanto segue corrisponde al vero (al meglio delle vostre capacità):

- la vostra valutazione è stata completa e accurata;
- al momento della compilazione, lo stato PCI DSS era accuratamente rappresentato, sia mediante la presentazione dell'Attestato di Conformità (AOC) o del Riepilogo Strumenti di approccio prioritario PCI (PAT) per la non conformità;
- siete autorizzati a rendere note le informazioni ivi contenute e fornite la Documentazione di convalida ad American Express senza violare alcun diritto di terzi.

Penali di mancata convalida e Risoluzione dell'Accordo

American Express ha il diritto di applicare nei vostri confronti penali di mancata convalida e risolvere l'Accordo se non soddisferete questi requisiti o se non fornirete ad American Express la Documentazione di convalida obbligatoria entro la data di scadenza stabilita. American Express proverà a notificare al referente per la sicurezza dei dati la data di scadenza stabilita per ciascun periodo di rendicontazione annuale e trimestrale.

Tabella A-4: Penali di mancata convalida

Descrizione*	Esercizio o Fornitore di servizi di 1° Livello	Esercizio o Fornitore di servizi di 2° Livello	Esercizio di 3° o 4° Livello
Verrà calcolata una penale di mancata convalida in caso di mancata ricezione della Documentazione di convalida entro la prima data di scadenza.	USD 25.000	USD 5.000	USD 50
Verrà calcolata una penale aggiuntiva di mancata convalida in caso di mancata ricezione della Documentazione di convalida entro la seconda data di scadenza.	USD 35.000	USD 10.000	USD 100
Verrà calcolata una penale di mancata convalida in caso di mancata ricezione della Documentazione di convalida entro la terza data di scadenza. **NOTA:** le penali di mancata convalida potranno continuare ad essere applicate fino a quando la documentazione di convalida non sarà trasmessa.	USD 45.000	USD 15.000	USD 250

* Le penali di mancata convalida saranno valutate in equivalenti in valuta locale.

* Non applicabile in Argentina.

Se gli obblighi dell'Esercizio relativi alla Documentazione di convalida PCI DSS non saranno soddisfatti, American Express avrà il diritto di imporre le penali di mancata convalida in modo cumulativo, trattenere pagamenti e/o porre termine all'Accordo.

Articolo 3 Oneri nella Gestione degli Incidenti con i dati

Siete tenuti a comunicare ad American Express eventuali Incidenti con i dati immediatamente, e comunque non oltre settantadue (72) ore dalla loro scoperta.

Per le comunicazioni ad American Express, contattate l'American Express Enterprise Incident Response Programme (*EIRP*) al numero telefonico gratuito +1.888.732.3750, oppure al +1.602.537.3021, oppure via e-mail all'indirizzo EIRP@aexp.com. L'Esercizio dovrà nominare un responsabile come suo contatto per la gestione del caso di Incidente con i dati. Inoltre:

- L'Esercizio dovrà condurre un'indagine approfondita su ogni Incidente con i dati e fornire prontamente ad American Express tutti numeri di Carta compromessi. American Express si riserva il diritto di condurre una propria analisi interna per identificare i numeri di Carta coinvolti nell'Incidente con i dati.

Per gli Incidenti con i dati che coinvolgono meno di 10.000 numeri di Carta univoci, un riepilogo dell'indagine deve essere fornito ad American Express entro dieci (10) giorni lavorativi dal suo completamento.

- I riepiloghi delle indagini devono contenere le seguenti informazioni: sintesi dell'incidente, descrizione dell'ambiente o degli ambienti interessati, cronologia degli eventi, date fondamentali, dettagli sull' incidenza e sull'esposizione dei dati, azioni di contenimento e di rimedio e attestazione che non vi sono elementi che indichino che altri dati American Express siano a rischio.

Per Incidenti con i dati che coinvolgano 10.000 o più numeri di Carta American Express univoci, siete tenuti a rivolgervi ad un Investigatore forense PCI (PFI), affinché conduca l'indagine entro cinque (5) giorni dalla scoperta dell'Incidente.

- Il rapporto di indagine legale originale andrà fornito ad American Express entro dieci (10) giorni lavorativi dal suo completamento.
- I rapporti di indagine legale devono essere compilati utilizzando il Modello di rapporto finale sull'incidente forense disponibile presso PCI. Tale rapporto dovrà includere le analisi legali, i rapporti sulla conformità e tutte le altre informazioni relative all'Incidente con i dati; identificare la causa dell'Incidente con i Dati; confermare se al momento dell'Incidente con i dati esisteva uno status di conformità con gli standard PCI DSS; e accertare la vostra capacità di prevenire futuri Incidenti con i dati mediante (i) la definizione di un piano di correzione di tutte le lacune riguardanti il PCI DSS e (ii) la partecipazione al programma di conformità American Express (come descritto più avanti). Su richiesta di American Express, dovrete ottenere da un Esperto qualificato in materia di valutazione della sicurezza (QSA) conferma di correzione delle lacune.

A prescindere da quanto esposto nei paragrafi precedenti di questo Articolo 3, "Oneri nella Gestione degli Incidenti con i dati":

- American Express può, a sua esclusiva discrezione, richiedervi di incaricare un PFI di condurre un'indagine in relazione a un Incidente con i dati che coinvolga meno di 10.000 numeri di Carta univoci o qualora siano avvenuti più Incidenti in un periodo di 12 mesi. Qualsiasi indagine di questo tipo dovrà essere conforme ai requisiti di cui sopra in questo Articolo 3, "Oneri nella Gestione degli Incidenti con i dati" e dovrà essere completata entro i tempi richiesti da American Express.
- American Express potrà, a sua esclusiva discrezione, rivolgersi separatamente a un PFI affinché conduca un'indagine per qualsiasi Incidente con i dati e potrà addebitarvene i costi.

L' Esercizio deve valutare l'Incidente con i dati in base alle leggi applicabili in materia di notifica delle violazioni dei dati a livello globale e, se ritenuto necessario, notificare le autorità di regolamentazione applicabili e i Titolari della Carta interessati in conformità con tali leggi di notifica delle violazioni dei dati. Se viene stabilito che il Fornitore di servizi o un'altra entità è responsabile della segnalazione dell'Incidente con i dati, l'Esercizio dovrà informare tale Fornitore di servizi o tale entità del suo dovere di valutare i propri obblighi di notifica ai sensi delle leggi applicabili in materia di notifica delle violazioni dei dati. Concordate di ottenere l'approvazione scritta di American Express prima di fare riferimento o citare American Express in qualsiasi comunicazione ai Titolari della Carta in merito all'Incidente con i dati. Concordate di collaborare con American Express nel fornire dettagli e risolvere tutti i problemi derivanti dall'Incidente con i dati, oltre che a fornire (e ottenere ogni deroga necessaria per effettuare tale fornitura di dati) ad American Express ogni informazione pertinente atta ad accertare la vostra capacità di prevenire futuri Incidenti con i dati in maniera conforme all'Accordo.

A prescindere da qualsivoglia obbligo di riservatezza diverso contenuto nell'Accordo, American Express ha il diritto di divulgare informazioni su qualsiasi Incidente con i Dati ai Titolari della Carta American Express , agli Emittenti, ad altri partecipanti alla rete American Express e al pubblico in generale, così come richiesto dalla Legge applicabile tramite ordinanza giudiziaria, amministrativa o normativa, decreto, invito a comparire, petizione o altro procedimento, allo scopo di attenuare il rischio di frode o qualsiasi altro danno; o altrimenti agire in misura adeguata al mantenimento dell'operatività della rete American Express.

Cosa fare in caso di Incidente con i dati?

L'Esercizio dovrà seguire queste fasi se identifica un Incidente con i dati all'interno della sua azienda.

Fase 1:

Compilare il Modulo di notifica iniziale di Incidente con i dati presso l'Esercizio e inviarlo via e-mail a EIRP@aexp.com entro 72 ore dalla scoperta dell'Incidente con i dati.

Fase 2:

Condurre un'indagine accurata; questa può richiedere che l'Esercizio incarichi un Investigatore forense per il settore Carte di pagamento (PCI).

Fase 3:

Fornire prontamente ad American Express tutti i numeri di Carta American Express® compromessi.

Fase 4:

Collaborare con American Express per aiutare a risolvere qualunque problema che emerga dall'Incidente con i dati.

Vedere Articolo 3, "Oneri nella Gestione degli Incidenti con i dati" per ulteriori dettagli sugli Oneri nella gestione degli Incidenti con i dati.

Ci sono ulteriori domande?

Stati Uniti: (888) 732-3750 (numero verde)

Altri Paesi: +1 (602) 537-3021

EIRP@aexp.com

Articolo 4 Oneri di Risarcimento per Incidenti con i dati

Gli oneri di risarcimento a vostro carico nei confronti di American Express stabiliti dall'Accordo per Incidenti con i dati sono determinati, senza alcuna deroga ad altri diritti e riparazioni di American Express, in base al presente Articolo 4, "Oneri di Risarcimento per Incidenti con i dati". Oltre agli oneri di risarcimento a vostro carico (se presenti), l'Esercizio potrebbe essere soggetto a una penale per mancata conformità alle disposizioni indicate in caso di Incidente con i dati, come descritte qui di seguito nel presente Articolo 4, "Oneri di Risarcimento per Incidenti con i dati".

Dovrete risarcire American Express con il valore di USD 5 per numero di Conto per Incidenti con i dati che riguardino:

- 10.000 o più numeri di Carta American Express con uno dei seguenti:
  - Dati sensibili di autenticazione, oppure
  - Data di scadenza

Tuttavia, American Express non richiederà alcun indennizzo per un Incidente con i dati che coinvolga:

- meno di 10.000 numeri di Carta American Express oppure
- più di 10.000 numeri di Carta American Express, se si verificano le seguenti condizioni:
  - l'Esercizio ha inviato a American Express notifica dell'Incidente con i dati seguendo le procedure indicate nell'Articolo 3, "Oneri nella Gestione degli Incidenti con i dati",
  - al momento in cui è avvenuto l'Incidente con i dati rispettavate le norme PCI DSS (se ciò viene confermato dall'indagine del PFI sull'Incidente con i Dati in oggetto), e
  - l'Incidente con i dati non era stato provocato da indebita condotta da parte vostra o delle Parti contemplate.

A prescindere da quanto stabilito nei paragrafi sopra esposti del presente Articolo 4, "Oneri di Risarcimento per Incidenti con i dati" per qualsivoglia Incidente con i dati, indipendentemente dal numero di Carte American Express coinvolte, sarà dovuta da parte vostra una penale ad American Express per il mancato rispetto delle disposizioni sugli Incidenti con i dati di importo fino a USD 100.000 per Incidente (come determinato da American Express a propria esclusiva discrezione) nel caso in cui non sia stato rispettato uno o più degli obblighi stabiliti nel precedente Articolo 3, "Oneri nella Gestione degli Incidenti con i dati". A scanso di equivoci, si specifica che l'importo totale della penale per la mancata conformità alle disposizioni in caso di Incidente con i dati non dovrà superare USD 100.000 ad Incidente.

American Express escluderà dal calcolo ogni numero di Conto American Express incluso in una precedente richiesta di indennizzo per Incidente con i dati avvenuto entro i dodici (12) mesi precedenti la Data di notifica. Tutti i calcoli eseguiti da American Express secondo questa formula sono definitivi.

Sulla base del presente Accordo, American Express potrà fatturarvi l'intero importo degli oneri di risarcimento per Incidenti con i dati da voi dovuti o detrarre tale importo dai pagamenti che American Express deve effettuare nei vostri confronti (o addebitare tale somma sul vostro conto corrente bancario).

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

A sua esclusiva discrezione, American Express potrà ridurre gli oneri di risarcimento solamente agli Esercizi che soddisfino tutti i requisiti seguenti:

- Prima dell'Incidente con i dati erano state implementate le Tecnologie di riduzione dei rischi applicabili e queste erano in uso durante l'intero arco temporale dell'Incidente stesso,
- È stata condotta e completata un'indagine approfondita di concerto con un PFI (salvo se diversamente concordato in precedenza per iscritto),
- Il rapporto legale afferma chiaramente che sono state utilizzate Tecnologie di riduzione dei rischi per elaborare, conservare e/o trasmettere i dati al momento dell'Incidente con i dati, e
- L'Esercizio non conserva (e non ha conservato durante l'intero arco temporale dell'Incidente con i dati) Dati sensibili di autenticazione o altri Dati del Titolare della Carta che non siano stati resi illeggibili.

Qualora sia disponibile una riduzione degli oneri di risarcimento per gli Esercizi (escludendo ogni penale di mancata conformità dovuta) questa sarà determinata nel modo seguente:

Tabella A-5: Criteri per la riduzione degli obblighi di risarcimento

Riduzione degli obblighi di risarcimento	Criteri richiesti
Riduzione standard: 50%	>75% delle transazioni totali elaborate su Dispositivi abilitati all'uso di Chip[1] OPPURE
	Tecnologia di riduzione dei rischi in uso in >75% delle sedi degli Esercizi[2]
Riduzione maggiorata: dal 75% al 100%	>75% di tutte le transazioni elaborate su Dispositivi abilitati all'uso di Chip[1] E altra Tecnologia di riduzione dei rischi in uso in >75% delle sedi degli Esercizi[2]

[1] Come determinato dall'analisi interna di American Express

[2] Come determinato da indagine PFI

- La riduzione maggiorata (dal 75% al 100%) sarà determinata in base al valore più basso riscontrato, espresso in percentuale, del numero di transazioni effettuate con Dispositivi abilitati all'uso di Chip E CONGIUNTAMENTE di sedi degli Esercizi che utilizzano un'altra Tecnologia di riduzione dei rischi. Gli esempi

della Tabella A-6: Aggiornamento della riduzione dell'obbligo di indennizzo illustrano il calcolo della riduzione del risarcimento.

- Perché un sistema tecnologico possa essere considerato una Tecnologia di attenuazione dei rischi, è necessario che l'Esercizio ne dimostri l'utilizzo efficace in conformità con la sua progettazione e il suo scopo previsto.
- La percentuale di vostre sedi che utilizzano una Tecnologia di riduzione dei rischi è determinata dall'indagine PFI.
- La riduzione degli oneri di risarcimento non si applica ad eventuali penali per mancata conformità esigibili in relazione all'Incidente.

Tabella A-6: Aggiornamento della riduzione dell'obbligo di indennizzo

Es.	Tecnologia di riduzione dei rischi in uso	Accettabile	Riduzione
1	• 80% delle transazioni su Dispositivi abilitati all'uso di Chip • 0% sedi che utilizzano un'altra Tecnologia di riduzione dei rischi	No	50%: Riduzione standard (meno del 75% di utilizzo di Tecnologie di riduzione dei rischi non configuri una Riduzione maggiorata)[1]
2	• 80% delle transazioni su Dispositivi abilitati all'uso di Chip • 77% sedi che utilizzano un'altra Tecnologia di riduzione dei rischi	Sì	77%: Riduzione maggiorata (in base al 77% di utilizzo di Tecnologia di riduzione dei rischi)
3	• 93% delle transazioni su Dispositivi abilitati all'uso di Chip • 100% sedi che utilizzano un'altra Tecnologia di riduzione dei rischi	Sì	93%: Riduzione maggiorata (in base al 93% delle transazioni su Dispositivi abilitati all'uso di Chip)
4	• 40% delle transazioni su Dispositivi abilitati all'uso di Chip • 90% sedi che utilizzano un'altra Tecnologia di riduzione dei rischi	No	50%: Riduzione standard (meno del 75% delle transazioni su Dispositivi abilitati all'uso di Chip non dà diritto a una Riduzione maggiorata)

[1] Un Incidente con i dati che coinvolga 10.000 Conti Carta American Express, al costo di USD 5,00 per numero di conto (10.000 x USD 5 = USD 50.000), può beneficiare di una riduzione del 50%, con un taglio degli oneri di risarcimento da USD 50.000 a USD 25.000, escluse eventuali penali per mancata conformità.

Articolo 5 Programma di analisi mirata (TAP)

La compromissione dei Dati del Titolare della Carta può essere causata da lacune nella sicurezza dei dati dell'Ambiente Dati del Titolare della Carta (CDE) dell'Esercizio.

Esempi di compromissione dei Dati del Titolare della Carta comprendono, ma non sono limitati a quanto segue:

- **Punto comune di acquisto (CPP):** i Titolari della Carta American Express comunicano che vi sono state transazioni fraudolente sul loro Conto Carta e queste sono state identificate e si determina che abbiano avuto origine da acquisti effettuati presso il Punto vendita dell'Esercizio.

- **Dati della Carta rilevati:** i Dati del Titolare della Carta e della Carta American Express sono stati trovati nel web collegati a Transazioni effettuate presso Punti vendita dell'Esercizio.
- **Sospetto di malware:** American Express sospetta che l'Esercizio stia utilizzando un software infetto con un codice vulnerabile o doloso.

Il TAP è stato progettato per identificare potenziali compromissioni dei dati del Titolare della Carta.

L'Esercizio dovrà conformarsi e dovrà far sì che tutti i soggetti di cui sia responsabile l'Esercizio stesso si conformino ai seguenti requisiti, in caso di notifica, da parte di American Express, di una potenziale compromissione dei Dati del Titolare della Carta.

- L'Esercizio dovrà prontamente rivedere il proprio CDE per rilevare eventuali falle nella sicurezza dei Dati e porvi rimedio.
  - L'Esercizio dovrà far sì che i suoi venditori terzi effettuino una accurata verifica del suo CDE se questo è realizzato in outsourcing.
- L'Esercizio dovrà fornire un sommario delle azioni intraprese o programmate per i suoi sforzi di verifica, valutazione e/o rimedio se richiesto da American Express.
- L'Esercizio dovrà fornire documenti aggiornati di convalida PCS DSS in accordo con l'Articolo 2, "Programma di conformità PCI DSS (Importante Convalida periodica dei Sistemi in uso)".
- A seconda di quanto applicabile, l'Esercizio dovrà incaricare un Investigatore forense PCI PFI qualificato perché esamini il suo CDE qualora lui o altri soggetti di cui sia responsabile:
  - Non riescano a risolvere la compromissione dei Dati del Titolare della Carta entro un periodo di tempo ragionevole, determinato da American Express, oppure
  - Confermino che si è verificato un Incidente con i dati e si conformino ai requisiti stabiliti nell'Articolo 3, "Oneri nella Gestione degli Incidenti con i dati".

Tabella A-7: Penali in caso di non conformità al TAP

Descrizione	Esercizio o Fornitore di servizi di 1° Livello	Esercizio o Fornitore di servizi di 2° Livello	Esercizio di 3° o 4° Livello
Potrebbe essere calcolata una penale di mancata convalida in caso di mancato soddisfacimento degli obblighi TAP entro la prima data di scadenza.	USD 25.000	USD 5.000	USD 1.000
Potrebbe essere calcolata una penale di mancata convalida in caso di mancato soddisfacimento degli obblighi TAP entro la seconda data di scadenza.	USD 35.000	USD 10.000	USD 2.500
Potrebbe essere calcolata una penale di mancata convalida in caso di mancato soddisfacimento degli obblighi TAP entro la terza data di scadenza. **NOTA:** *le penali di mancata convalida potranno continuare ad essere applicate fino a quando gli obblighi non saranno soddisfatti o il TAP non sarà risolto.*	USD 45.000	USD 15.000	USD 5.000

Se gli obblighi dell'Esercizio previsti dal TAP non saranno soddisfatti, American Express avrà il diritto di imporre gli Oneri di non conformità in modo cumulativo, trattenere pagamenti e/o porre termine all'Accordo.

Articolo 6 Riservatezza

American Express adotterà ogni precauzione ragionevole per mantenere la riservatezza (e esigerla dai propri agenti e subappaltatori, compresa il fornitore del Portale) 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:

a. sia già nota ad American Express prima della divulgazione;

b. sia o diventi di pubblico dominio in assenza di violazione del presente Comma da parte di American Express;

c. sia debitamente consegnata a terzi da American Express senza alcun obbligo di riservatezza;

d. sia sviluppata in maniera indipendente da American Express; oppure

e. debba essere divulgata a seguito di un'ordinanza da parte di un tribunale, un ente amministrativo o un'autorità governativa, ovvero per legge, norma o regolamento oppure a seguito di invito a comparire, richiesta di presentazione, 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 (compresi enti di controllo, di ispezione, di medicina legale o agenzia delle forze dell'ordine).

Articolo 7 Dichiarazione di non responsabilità

AMERICAN EXPRESS DISCONOSCE QUALSIASI DICHIARAZIONE, GARANZIA E RESPONSABILITÀ IN RELAZIONE ALLA PRESENTE PROCEDURA OPERATIVA DI SICUREZZA DEI DATI, CONCERNENTI IL PCI DSS, LE SPECIFICHE EMV E LA DESIGNAZIONE E L'OPERATO DI QSA, ASV O PFI (O DI OGNUNA DI QUESTE FIGURE), IN FORMA ESPLICITA, IMPLICITA, REGOLAMENTARE O DI QUALSIASI ALTRO TIPO, INCLUSA QUALSIASI GARANZIA DI COMMERCIABILITÀ O IDONEITÀ PER UNO SCOPO SPECIFICO. AI TERMINI DELLA PRESENTE PROCEDURA, LE SOCIETÀ EMITTENTI DI CARTA AMERICAN EXPRESS NON SONO TERZE PARTI BENEFICIARIE.

Articolo 8 Definizioni

Ai fini esclusivi di questa *Procedura operativa di sicurezza dei dati* si applicano e prevalgono in caso di conflitto tra i termini le definizioni riportate nelle *Norme per gli Esercizi Convenzionati*.

Accredito indica l'importo dell'Addebito rimborsato ai Titolare della Carta per acquisti o pagamenti effettuati con la Carta.

Accordo indica le Disposizioni generali, le Norme per gli Esercizi Convenzionati e tutti gli allegati e le schede che li accompagnano (talvolta indicati come Accordo di accettazione della Carta nella nostra documentazione).

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

Affiliante indica l'operatore di un Esercizio commerciale che autorizza altre persone o Entità (Affiliati) a distribuire beni e/o servizi o ad operare con il marchio dell'operatore; che fornisce assistenza agli Affiliati nello svolgimento delle proprie attività o influenza il metodo di operatività dell'Affiliato; e che richiede il pagamento di una quota da parte degli Affiliati.

Affiliato indica una terza parte indipendente sia come gestione che come titolarità (compreso un affiliato, un licenziatario o un ramo di impresa) diverso da una Affiliata, che opera con licenza da parte di un Affiliante per gestire un franchising e che ha stipulato un accordo scritto con l'Affiliante, in cui esibisce costantemente una identificazione esterna, che si identifica sostanzialmente con i marchi dell'Affiliante o si presenta al pubblico come membro del gruppo aziendale dell'Affiliante.

Ambiente Dati del Titolare della Carta (CDE) indica il personale, i processi e le tecnologie che memorizzano, elaborano o trasmettono dati del Titolare della Carta o dati di autenticazione sensibile dello stesso.

Applicazione per il pagamento ha il significato attribuitogli nelle Definizioni correnti dei termini per il Secure Software Standard e il Secure Software Life Cycle Standard, disponibili all'indirizzo 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) compaiono, al momento della loro commercializzazione, nell'elenco delle società e dei fornitori approvati gestito da PCI Security Standards Council, LLC, che è disponibile sul sito www.pcisecuritystandards.org.

Arco temporale dell'Incidente con i dati indica l'intervallo di tempo (o un periodo di tempo determinato in modo analogo) di intromissione indicato nel rapporto forense finale (ad esempio, rapporto PFI) o, se sconosciuto, fino a 365 giorni prima dell'ultima Data di notifica dei numeri di Carta potenzialmente compromessi coinvolti in un incidente segnalata ad American Express.

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

Attestato di conformità della scansione (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.

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 ancora indica un numero di conto Carta.

Carta con Chip indica una Carta contenente un Chip che può richiedere un PIN come strumento di verifica dell'identità del Titolare della Carta 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").

Chiave crittografica ("chiave crittografica American Express") indica tutte le chiavi usate nell'elaborazione, creazione, caricamento e/o protezione dei dati sul conto. Queste comprendono, ma non sono limitate a quanto segue:

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

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

Cliente indica un Titolare della Carta che acquista beni, servizi o entrambi.

Crittografia Point-to-Point Encryption (P2PE) indica una soluzione che protegge mediante crittografia i dati relativi a un conto dal punto in cui un Esercizio accetta la Carta di pagamento al punto protetto di decrittografia.

Data di notifica indica la data in cui American Express fornisce alle società emittenti la notifica finale di un Incidente con i dati. Tale data è subordinata alla ricezione da parte di American Express del rapporto forense finale o dell'analisi interna e sarà stabilita a discrezione esclusiva di American Express.

Dati del Conto indica i Dati del Titolare della Carta e/o i dati sensibili di autenticazione. Vedere Dati del Titolare della Carta e Dati sensibili di autenticazione.

Dati del Titolare della Carta indica il Numero di conto principale (PAN) completo di per sé o il PAN completo più uno dei seguenti dati: nome del Titolare della Carta, data di scadenza e/o codice del servizio. Vedere Dati sensibili di autenticazione per ulteriori informazioni sui dati che potrebbero essere trasmessi o elaborati (ma non conservati) nell'ambito di una transazione di pagamento.

Dati della transazione indica tutte le informazioni richieste da American Express, comprovanti una o più transazioni, comprese le informazioni ottenute presso il Punto vendita, le informazioni ottenute o generate durante l'Autorizzazione e la Trasmissione, e qualsiasi Storno di Addebito.

Dati sensibili di autenticazione indica le informazioni relative alla sicurezza utilizzate per autenticare i Titolari della Carta e/o autorizzare le transazioni con carta di pagamento. Queste informazioni includono, a titolo esemplificativo ma non esaustivo, i codici di verifica della Carta, i dati completi della striscia magnetica o i dati equivalenti su un chip, i PIN e i blocchi PIN.

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.

Dispositivo per il pagamento con immissione di PIN ha lo stesso significato attribuitogli dalle Definizioni correnti dei termini per la sicurezza delle transazioni con PIN abituali nel settore per le Carte di pagamento (PTS), Punto di interazione (POI), Requisiti di sicurezza modulare, disponibili sul sito www.pcisecuritystandards.org.

Documento di Addebito indica una documentazione riproducibile (sia cartacea che elettronica) di un Addebito conforme ai nostri requisiti e contenente il Numero della Carta, la data della transazione, l'importo in dollari, l'Approvazione, la firma del Titolare (se applicabile) e altre informazioni.

Documento di Credito indica una documentazione di Accredito che soddisfa i requisiti di American Express.

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 annuale del Programma STEP.

Emittente della Carta indica qualunque Entità (compresa American Express e i suoi affiliati) autorizzata da American Express o da un Affiliato di American Express ad emettere Carte e ad impegnarsi nell'attività di emissione di Carte.

Esercizio indica l'Esercizio e tutti i suoi affiliati che accettano Carte American Express secondo un Accordo con American Express o le sue affiliate.

Esercizio di 1° Livello indica un Esercizio che effettua almeno 2,5 milioni di transazioni con Carta American Express per anno; oppure qualsiasi Esercizio che American Express designi come di 1° Livello.

Esercizio di 2° Livello indica un Esercizio che effettua da 50.000 a meno di 2,5 milioni di transazioni con Carta American Express all'anno.

Esercizio di 3° Livello indica un Esercizio che effettua da 10.000 a meno di 50.000 milioni di transazioni con Carta American Express all'anno.

Esercizio di 4° Livello indica un Esercizio che effettua meno di 10.000 transazioni con Carta American Express all'anno.

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

Fornitore di prodotti di scansione approvato (ASV) indica una Persona 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.

Fornitori di servizi indica i responsabili delle elaborazioni autorizzati, i responsabili delle elaborazioni di terzi, i fornitori di gateway, gli integratori di terminali POS e qualsiasi altro fornitore per Esercizi di terminali POS o di altre soluzioni o servizi per l'elaborazione dei pagamenti.

Fornitore di servizi di 1° Livello Indica un Fornitore di servizi con almeno 2,5 milioni di transazioni con Carta American Express all'anno; oppure qualsiasi Fornitore di servizi che American Express designi come di 1° Livello.

Fornitore di servizi di 2° Livello Indica un Fornitore di servizi con meno di 2,5 milioni di transazioni con Carta American Express all'anno; oppure qualsiasi Fornitore di servizi non ritenuto di 1° Livello da American Express.

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

- accesso o utilizzo non autorizzato di Chiavi di Crittografia, Dati del Titolare della Carta o Dati sensibili di autenticazione (o una combinazione di questi) che vengono memorizzati, elaborati o trasmessi su apparecchiature, sistemi e/o reti (o sui relativi componenti) dell'utente o l'uso dei quali è richiesto obbligatoriamente o fornito o reso disponibile dall'Esercizio;

- utilizzo di tali Chiavi di Crittografia, Dati del Titolare della Carta o Dati di autenticazione sensibili (o una combinazione di questi) diversi da quelli previsti dall'Accordo; e/o
- la perdita, il furto o l'appropriazione indebita presunta o acclarata di qualsiasi mezzo, materiale, registro o informazione contenente Chiavi di crittografia, Dati del Titolare della Carta o Dati sensibili di autenticazione (o una combinazione di questi).

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

Investigatore forense PCI (PFI) indica una persona fisica o giuridica autorizzata dal Payment Card Industry Security Standards Council, LLC alla conduzione di indagini forensi su una violazione o una compromissione dei dati di una Carta di pagamento.

Livello dell'Esercizio indica la classificazione che American Express assegna agli Esercizi relativamente ai loro obblighi di convalida della conformità al PCI DSS, come descritto nell'Articolo 2, "Programma di conformità PCI DSS (Importante Convalida periodica dei Sistemi in uso)".

Modello di relazione forense finale per gli incidenti indica il modello disponibile presso il PCI Security Standards Council, sul sito www.pcisecuritystandards.org.

Numero della Carta indica il numero unico di identificazione che l'Emittente assegna alla Carta al momento dell'emissione.

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

Numero di conto principale (PAN) ha il significato attribuitogli nell'allora corrente glossario dei termini per PCI DSS.

Parti contemplate indica tutti i dipendenti, gli agenti, i rappresentanti, i subappaltatori, i Responsabili dell'elaborazione, i Fornitori di servizi, i fornitori di terminali POS o di sistemi o di soluzioni per l'elaborazione dei pagamenti, Entità associate al conto Esercizio American Express, e chiunque altro a cui possa essere fornito l'accesso ai Dati sul Titolare della Carta o ai Dati di Autenticazione sensibili (o a entrambi) conformemente all'Accordo.

Payment Card Industry Data Security Standard (PCI DSS) indica il Payment Card Industry Data Security Standard, disponibile sul sito www.pcisecuritystandards.org.

PCI DSS indica il Payment Card Industry Data Security Standard, disponibile sul sito www.pcisecuritystandards.org.

Portale, Il indica il sistema di comunicazione fornito dall'amministratore del Programma PCI di American Express scelto da American Express. Esercizi e Fornitori di servizi devono utilizzare il Portale per trasmettere la documentazione di convalida PCI ad American Express.

Programma, Il indica il Programma di conformità PCI di American Express.

Programma di analisi mirata indica un programma che permette la rapida identificazione di una potenziale compromissione dei dati del Titolare della Carta nell'Ambiente Dati del Titolare della Carta (CDE). Vedere Articolo 5, "Programma di analisi mirata (TAP)".

Programma Security Technology Enhancement (STEP) indica il programma di American Express in cui gli Esercizi sono incoraggiati a mettere in atto tecnologie che migliorino la sicurezza dei dati.

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

Requisiti del Payment Card Industry Security Standards Council (PCI SSC) indica l'insieme di standard e requisiti relativi alla sicurezza e alla protezione dei dati delle carte di pagamento, inclusi gli standard PCI DSS e PA DSS e disponibile sul sito www.pcisecuritystandards.org.

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

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

Soluzione P2PE (Point-to-Point Encryption) approvata, è una soluzione inclusa in un elenco PCI SSC di soluzioni convalidate oppure è convalidata da un esperto qualificato in materia di valutazione della sicurezza PCI SSC o da una società di P2PE.

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

Tecnologia di riduzione dei rischi indica le soluzioni tecnologiche che migliorano la sicurezza dei Dati del Titolare della Carta American Express e dei Dati sensibili di autenticazione, come stabilito da American Express. Perché una Tecnologia di riduzione dei rischi possa essere ammissibile, occorre dimostrare che il suo utilizzo effettivo è conforme ai propositi e agli scopi previsti. A titolo di esempio, ma senza limitarsi ad essi, citiamo: EMV, crittografia P2PE e tokenizzazione.

Terminale 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 Esercizio per ottenere autorizzazioni e/o per raccogliere dati sulle transazioni o entrambe le cose.

Titolare della Carta 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 compare sulla Carta.

Titolare della Carta indica un cliente a cui è stata emessa una carta di pagamento, o qualsiasi persona autorizzata a utilizzare la carta di pagamento.

Token indica il token criptografico che sostituisce il PAN, basandosi su un determinato indice per un valore non prevedibile.

Transazione indica un Addebito, un Accredito, un Anticipo di contante (o altro accesso al contante) o una transazione ATM completata per mezzo di una Carta.

Transazione Buyer Initiated Payment (BIP) indica una soluzione digitale di pagamento che consente agli acquirenti di programmare in modo rapido ed efficiente i pagamenti ai fornitori (collegati alle carte aziendali).

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") effettuata 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 www.emvco.com.

Articolo 9 Siti web utili

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

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

EMVCo: www.emvco.com