AMERICAN EXPRESS

Procedura operativa di sicurezza dei dati (DSOP)

Icone di modifica

Gli aggiornamenti importanti sono elencati nella Tabella di Riepilogo delle modifiche, e indicati inoltre nella *DSOP* con un'icona di modifica. Un'icona di modifica accanto al titolo di un Articolo o di un Comma indica un testo revisionato, aggiunto o rimosso da tale Articolo o Comma. Le modifiche nella *DSOP* sono indicate con una icona di modifica come riportato qui.

Tabella di riepilogo delle modifiche

Gli aggiornamenti importanti sono elencati nella seguente tabella e indicati inoltre nella *DSOP* con un'icona di modifica.

Articolo/Comma	Descrizione della modifica
Articolo 1, "Programma di analisi mirata (TAP)"	• Rinominato l'Articolo 1 da Compromissione dei Dati del Titolare in Programma di analisi mirata (TAP). • Chiarito il linguaggio.
Definizioni	• Aggiornato il linguaggio per gli Incidenti con i dati. • Aggiunte definizioni per Ambiente dati del Titolare della Carta e Programma di analisi mirata.

American Express, società leader nella tutela dei propri utenti, è da tempo impegnata nella protezione dei Dati dei Titolari di 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 di seguito con il termine l'Accordo) e la presente Procedura operativa di sicurezza dei dati, 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.

Articolo 1 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 pericoloso.

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 5, "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".

Oneri 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
Oneri di non conformità calcolati qualora gli obblighi di gestione previsti dal TAP non vengano soddisfatti entro 45 giorni dalla data di notifica.	USD 25.000	USD 5.000	USD 1.000
Oneri di non conformità calcolati qualora gli obblighi di gestione previsti dal TAP non vengano soddisfatti entro 90 giorni dalla data di notifica.	USD 35.000	USD 10.000	USD 2.500
Oneri di non conformità calcolati qualora gli obblighi di gestione previsti dal TAP non vengano soddisfatti entro 120 giorni dalla data di notifica. **NOTA:** *Gli oneri di non conformità potranno continuare ad essere applicati mensilmente fino a quando gli obblighi non saranno soddisfatti o sarà completato il TAP.*	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 2 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 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 degli altri Requisiti del Payment Card Industry Security Standards Council (PCI SSC) applicabili per le vostre operazioni di elaborazione, conservazione e trasmissione dei Dati del Titolare della Carta o dei Dati sensibili di autenticazione entro la 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, nelle sedi presidiate, solo quelli approvati dalla PCI.

Siete tenuti a proteggere tutta la documentazione di Addebito e Accredito 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 5, "Importante Convalida periodica dei Sistemi in uso", a meno che sia presente diversa disposizione in tale articolo).

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 +1 (602) 537-3021 (il segno + indica il prefisso di chiamata internazionale diretta o "IDD"; tariffazione internazionale applicabile), o via email all'indirizzo di posta elettronica EIRP@aexp.com. L'Esercizio dovrà nominare un responsabile come suo contatto per la gestione del caso di Incidente con i dati. Inoltre:

- Siete tenuti a condurre un'indagine legale accurata su ciascun Incidente con i dati.
- Per Incidenti con i dati che coinvolgano 10.000 o più numeri di conto Carta American Express unici, 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.
- Siete tenuti a fornire prontamente ad American Express tutti i 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.

I rapporti di indagine legale dovranno essere compilati utilizzando l'attuale Modello di rapporto finale legale per gli Incidenti (Forensic Incident Final Report Template) messo a disposizione dal PCI. Tale rapporto dovrà includere esami forensi, relazioni sulla conformità e ogni altra informazione relativa all'Incidente con i dati; dovrà identificare la causa dell'Incidente con i dati; confermare se rispettavate il PCI DSS al momento dell'Incidente con i dati; 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 potrà, a sua esclusiva discrezione, richiedere all'utente di incaricare un PFI di condurre un'indagine su un Incidente con i dati per Incidenti con i dati che coinvolgano meno di 10.000 numeri di Carta unici. 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.

Concordate di collaborare con American Express alla risoluzione di tutti i problemi derivanti dall'Incidente con i dati, oltre che a consultarvi con American Express riguardo alle informazioni da fornire ai Titolari di Carta American Express coinvolti nell'Incidente con i dati e 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 di Carte 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.

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 potreste essere soggetti 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".

In caso di Incidenti con i Dati, che coinvolgano:

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

  dovrete risarcire American Express con il valore di USD 5 per numero di conto.

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:
  - avete fornito ad American Express notifica dell'Incidente con i dati seguendo le procedure indicate nel presente Articolo 4, "Oneri di Risarcimento per 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 Carta 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 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 forense 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:

Riduzione degli oneri 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] Determinata da un'analisi interna di American Express

[2] Determinata 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 riportati di seguito illustrano il calcolo della riduzione del risarcimento.
- 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. Ad esempio, dotarsi di Dispositivi abilitati all'uso di Chip e poi elaborare le transazioni con Carte con Chip sfruttandone la banda magnetica o l'inserimento manuale del dato Carta NON è considerato un utilizzo efficace di questa Tecnologia.
- 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.

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

Es.	Tecnologia di riduzione dei rischi in uso	Accettabile	Riduzione
4	40% delle transazioni su Dispositivi abilitati all'uso di Chip	No	50%: Riduzione standard (meno del 75% delle transazioni su Dispositivi abilitati all'uso di Chip non dà diritto a una Riduzione maggiorata)
	90% sedi che utilizzano un'altra Tecnologia di riduzione dei rischi		

[1] Un Incidente con i dati che coinvolga 10.000 conti Carta American Express, al costo di USD 5 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 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) 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 American Express ai sensi della presente procedura.

Azione 2: Riconoscimento del proprio Livello e dei Requisiti 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 1° e 2° Livello e tutti i Fornitori di servizi, secondo la definizione fornita a seguire, dovranno partecipare al programma di conformità PCI American Express ai sensi della presente procedura 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 SecureTrust, divisione di Trustwave (https://portal.securetrust.com), che amministra il programma per conto di American Express, secondo uno dei metodi elencati alla Azione 4: "Invio della Documentazione di convalida ad American Express" in seguito descritto. Siete tenuti a comunicare a SecureTrust qualsiasi variazione di queste informazioni, fornendo all'occorrenza i dati aggiornati. Il mancato conferimento da parte dell'utente di tali informazioni di contatto non influirà sul nostro diritto di stabilire le penali per la mancata convalida come indicato nella Tabella delle penali di mancata convalida.

American Express può richiedere, a sua esclusiva discrezione, ad alcuni Esercizi di 3° e 4° Livello di partecipare al programma di conformità American Express ai sensi della presente procedura inviando loro comunicazione scritta. L'Esercizio dovrà iscriversi entro e non oltre 90 giorni dalla ricezione della comunicazione.

Azione 2: Riconoscimento del proprio Livello e dei Requisiti 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. Nel caso degli Esercizi, questo corrisponde al volume inoltrato dai propri Punti vendita e aggregato al massimo livello di Esercizio American Express.* Rientrerete in uno in uno dei Livelli specificati nelle tabelle Esercizi e Fornitori di servizi illustrate più avanti. 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.

* Nel caso degli Affillianti, è incluso il volume degli Esercizi dei 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.

Requisiti per gli Esercizi

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

- **Esercizio di 1° Livello** – Almeno 2,5 milioni di transazioni 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 2,5 milioni di transazioni con Carta American Express all'anno.
- **Esercizio di 3° Livello** – Da 10.000 a 50.000 transazioni con Carta American Express all'anno.
- **Esercizio di 4° Livello** – Meno di 10.000 transazioni con Carta American Express all'anno.

Tabella Esercizi

	Documentazione di convalida		
Livello dell'Esercizio/ transazioni annuali con Carta American Express	Relazione di valutazione sulla conformità in loco (ROC)	Questionario di autovalutazione (SAQ) e Scansione di rete trimestrale	Attestato STEP per gli Esercizi qualificati a partecipare al programma
Livello 1/ 2,5 milioni o più	Obbligatorio	Non applicabile	Facoltativo (sostituisce il ROC)
Livello 2/ da 50.000 a 2,5 milioni	Facoltativo	SAQ obbligatorio (salvo presentazione di una valutazione in loco); scansione obbligatoria con certi tipi di SAQ	Facoltativo (sostituisce il SAQ e la Scansione di rete o il ROC)
Livello 3/ da 10.000 a 50.000	Facoltativo	SAQ facoltativo (obbligatorio se richiesto da American Express); scansione obbligatoria con certi tipi di SAQ	Facoltativo (sostituisce il SAQ e la Scansione di rete o il ROC)
Livello 4/ 10.000 o meno	Facoltativo	SAQ facoltativo (obbligatorio se richiesto da American Express); scansione obbligatoria con certi tipi di SAQ	Facoltativo (sostituisce il SAQ e la Scansione di rete o il ROC)

* 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 l'accuratezza e l'adeguatezza della Documentazione di convalida PCI fornita secondo necessità, anche coinvolgendo, a spese di American Express, un QSA o PFI di propria scelta.

Programma Security Technology Enhancement (STEP)

A discrezione di American Express, gli Esercizi che sono conformi al PCI DSS possono anche 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 è valido 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:

- **EMV** – 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

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".

Requisiti per i Fornitori di servizi

I Fornitori di servizi (non Esercizi) rientrano in una tra 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 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 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.

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

Tabella Fornitori di servizi

Livello	Documentazione di convalida	Requisito
1	Relazione annuale di valutazione della sicurezza sulla conformità in loco	Obbligatorio
2	SAQ D annuale (Fornitore di servizi) e Scansione di rete trimestrale oppure Relazione annuale di valutazione della sicurezza sulla conformità in loco, se preferibile	Obbligatorio

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

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

La seguente documentazione è richiesta ai diversi livelli di Esercizio 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 effettuata 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 annuale ad American Express con l'Attestato di conformità (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 (Esercizi e Fornitori di servizi di 1° Livello).

Questionario di autovalutazione annuale – L'Autovalutazione annuale è un processo basato sul PCI DSS 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 (o entrambi). Deve essere compilato da voi e certificato 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 annuale 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 (Esercizi di 2°, 3° e 4° Livello; Fornitori di servizi di 2° Livello).

Scansione di rete trimestrale – La Scansione di rete trimestrale è un processo che da 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 autorizzato (**ASV**). Siete tenuti a compilare e inviare su base trimestrale ad American Express l'Attestato di conformità della scansione (**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 (per tutti gli Esercizi ad eccezione di quelli che presentano anche una Relazione di valutazione della sicurezza in loco e di quelli qualificati a partecipare al programma STEP; per tutti i Fornitori di servizi). A scanso di qualsiasi equivoco, si sottolinea che le Scansioni di rete trimestrali sono obbligatorie se richieste dal SAQ applicabile.

Documentazione di convalida dell'attestato annuale del Programma STEP – L'attestato di qualifica annuale del Programma STEP ("Attestato STEP") di American Express è a disposizione solo degli Esercizi che soddisfano i requisiti elencati nella Azione 2: "Riconoscimento del proprio Livello e dei Requisiti di convalida" esposto sopra. L'Attestato STEP implica un processo basato sui requisiti PCI DSS 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 (o entrambi). Deve essere compilato da voi e certificato dal vostro amministratore delegato, direttore amministrativo e finanziario, responsabile della sicurezza delle informazioni aziendali o direttore. A completamento della procedura dovrete inviare ogni anno il modulo dell'Attestato STEP ad American Express. (Solo Esercizi qualificati a partecipare al programma STEP). Il modulo dell'Attestato annuale del Programma STEP può essere scaricato dal portale protetto SecureTrust.

Mancata conformità al PCI DSS – Se risulta che non siete in conformità con il PCI DSS, siete tenuti a fornire uno dei seguenti documenti:

- un Attestato di conformità (AOC) comprendente la "Parte 4. Piano di azione per Status di non conformità"
- un Riepilogo e attestato di conformità dei tool utilizzati per raggiungere i requisiti PCI (PASAOC)
- un modello di Piano di progetto (scaricabile nel portale protetto SecureTrust)

Ciascuno dei succitati documenti dovrà indicare una data per il termine della riparazione, non superiore a 12 mesi successivi alla data di compilazione della documentazione, al fine di garantire la conformità ai termini stabiliti. La documentazione appropriata andrà trasmessa ad American Express secondo uno dei metodi elencati nella Azione 4: "Invio della Documentazione di convalida ad American Express" come in seguito descritto. Dovrete fornire ad American Express aggiornamenti periodici sullo stato di attuazione della procedura di riparazione del vostro Status di non conformità (Esercizi di 1°, 2°, 3° e 4° Livello; tutti i Fornitori di servizi). A scanso di qualsiasi equivoco, gli Esercizi non conformi al PCI DSS non saranno qualificati a partecipare al Programma STEP. American Express non applicherà nei vostri confronti le penali di mancata convalida (descritte più avanti) prima della data di termine della riparazione, 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 procedura.

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 American Express di conformità PCI sono tenuti a consegnare la Documentazione di convalida indicata come "obbligatoria" nelle tabelle illustrate nella Azione 2: "Riconoscimento del proprio Livello e dei Requisiti di convalida". La Documentazione di convalida andrà inviata a SecureTrust mediante uno dei seguenti metodi:

- **Portale protetto**: La Documentazione di convalida può essere caricata nel portale protetto SecureTrust sul sito https://portal.securetrust.com.

  Per istruzioni sull'utilizzo di questo portale, contattare SecureTrust al numero telefonico del vostro Paese oppure via email all'indirizzo di posta elettronica americanexpresscompliance@securetrust.com.
- **Fax protetto**: La Documentazione di convalida può essere inviata per 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 Esercizi, il numero Esercizio American Express di 10 cifre.

Per domande generali sul programma o sul processo descritto in precedenza, contattare SecureTrust al numero + 800 9000 1140 o +1 (312) 267-3208 o via email all'indirizzo di posta elettronica americanexpresscompliance@securetrust.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 terza parte.

Paese	Numero telefonico SecureTrust
Argentina	+ 800 9000 1140
Australia	+ 800 9000 1140
Austria	+ 800 9000 1140
Bulgaria	+ 312 267 3208
Canada	1 866 659 9016
Cipro	+ 800 9000 1140
Croazia	+ 312 267 3208
Danimarca	+ 800 9000 1140
Estonia	+ 312 267 3208
Francia	+ 800 9000 1140
Germania	+ 800 9000 1140
Giappone	+ 312 267 3208
Grecia	+ 312 267 3208
Hong Kong	+ 800 9000 1140

Paese	Numero telefonico SecureTrust
IDC	+ 888 900 0114
India	+ 000 800 100 1177
Irlanda	+ 800 9000 1140
Islanda	+ 800 9000 1140
Italia	+ 800 9000 1140
Lettonia	+ 312 267 3208
Lituania	+ 312 267 3208
Malta	+ 312 267 3208
Messico	+ 888 900 0114
Norvegia	+ 800 9000 1140
Nuova Zelanda	+ 800 9000 1140
Paesi Bassi	+ 312 267 3208
Polonia	+ 800 9000 1140
Portogallo	+ 312 267 3208
Regno Unito	+ 800 9000 1140
Repubblica Ceca	+ 800 144 316
Romania	+ 312 267 3208
Russia	+ 312 267 3208
Singapore	+ 800 9000 1140
Slovacchia	+ 312 267 3208
Slovenia	+ 312 267 3208
Spagna	+ 800 9000 1140
Stati Uniti	1 866 659 9016
Svezia	+ 800 9000 1140
Taiwan	+ 312 267 3208
Thailandia	+ 800 9000 1140
Ungheria	+ 800 9000 1140

il segno + indica un prefisso di chiamata internazionale diretta o “IDD”; tariffazione internazionale applicabile

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 provvederà a comunicarvi separatamente la data di scadenza stabilita per ciascun periodo di rendicontazione annuale e trimestrale.

Inviate la documentazione ad American Express entro la scadenza prevista. American Express provvederà a comunicarvi separatamente la data di scadenza stabilita per ciascun periodo di rendicontazione annuale e trimestrale.

Tabella delle 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 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 un'ulteriore penale in caso di mancata ricezione della Documentazione di convalida entro 60 giorni dalla prima data di scadenza.	USD 35.000	USD 10.000	USD 100
Verrà calcolata un'ulteriore penale in caso di mancata ricezione della Documentazione di convalida entro 90 giorni dalla prima data di scadenza, e ogni 30 giorni successivi.	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 American Express non riceverà la Documentazione di convalida obbligatoria entro 90 giorni dalla prima data di scadenza, avrà il diritto di risolvere l'Accordo conformemente ai termini previsti e di applicare in maniera cumulativa nei vostri confronti le precedenti penali di mancata convalida.

Articolo 6 Riservatezza

American Express adotterà ogni precauzione ragionevole per mantenere la riservatezza (e esigerla dai propri agenti e subappaltatori, compresa SecureTrust) 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.

Siti web utili

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

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

Definizioni

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

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

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 lo stesso significato attribuitole dalle Definizioni correnti dei termini del Payment Card Industry Payment Application Data Security Standard, disponibile sul sito 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 che ha inizio alla data della compromissione, se nota, ovvero 365 giorni prima della Data di notifica se la data effettiva della compromissione non è nota. L'arco temporale dell'Incidente con i dati termina 30 giorni dopo la Data di notifica.

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.

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 Titolare della Carta ha lo stesso significato attribuitogli dalle Definizioni correnti dei termini del PCI DSS.

Dati sensibili di autenticazione ha lo stesso significato attribuito al termine dalle Definizioni correnti dei termini del PCI DSS.

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.

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 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 2,5 milioni di transazioni con Carta American Express all'anno.

Esercizio di 3° Livello indica un Esercizio che effettua da 10.000 a 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.

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.

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 alle Informazioni sul Titolare della Carta 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.

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 1, "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. Per essere ammessi al Programma STEP, gli Esercizi non devono essere incorsi in alcun Incidente con i dati nei 12 mesi precedenti la presentazione dell'Attestato STEP annuale e devono elaborare almeno il 75% di tutte le transazioni mediante crittografia P2PE oppure con EMV su Dispositivi abilitati all'uso di Chip.

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. Tra gli esempi figurano: 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.

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

Transazione Buyer Initiated Payment (BIP) indica una transazione di pagamento resa possibile mediante un archivio di istruzioni di pagamento elaborato con procedura BIP, ovvero avviata dall'acquirente.

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.