

# Πολιτική Λειτουργίας Ασφάλειας Δεδομένων (DSOP)

## Γραμμές αλλαγής

Οι σημαντικές επικαιροποιήσεις αναφέρονται στον Πίνακα Περίληψης Αλλαγών και επισημαίνονται επίσης στην DSOP με μια γραμμή αλλαγής. Οι γραμμές αλλαγής είναι κατακόρυφες γραμμές στο αριστερό περιθώριο οι οποίες υποδεικνύουν την αναθεώρηση, την προσθήκη ή τη διαγραφή κειμένου. Όλες οι αλλαγές στην DSOP υποδεικνύονται με μια γραμμή αλλαγής όπως φαίνεται εδώ.



## Πίνακας Περίληψης Αλλαγών

Οι σημαντικές επικαιροποιήσεις αναφέρονται στον παρακάτω πίνακα και επισημαίνονται επίσης στην DSOP με μια γραμμή αλλαγής.

Ενότητα/Υποενότητα	Περιγραφή αλλαγής
Δεν υπάρχουν αλλαγές σε αυτήν την έκδοση.	

## Τι πρέπει να κάνετε εάν προκύψει Περιστατικό Παραβίασης Δεδομένων;

Ακολουθήστε αυτά τα βήματα εάν εντοπίσετε κάποιο Περιστατικό Παραβίασης Δεδομένων στην επιχείρησή σας.



### Βήμα 1:

Συμπληρώστε το [Έντυπο Αρχικής Ειδοποίησης Σχετικά με Περιστατικό Παραβίασης Εμπορικών Δεδομένων](#) και αποστείλετέ το μέσω email στη διεύθυνση [EIRP@aexp.com](mailto:EIRP@aexp.com) εντός 72 ωρών μετά την ανακάλυψη του Περιστατικού Παραβίασης Δεδομένων.



### Βήμα 2:

Διεξαγάγετε διεξοδική έρευνα. Για την έρευνα ενδέχεται να χρειαστεί η πρόσληψη [Εγκληματολογικού Ερευνητή Καρτών Πληρωμής \(Payment Card Industry, PCI\)](#).



### Βήμα 3:

Προσκομίστε μας εγκαίρως όλους τους αριθμούς Καρτών American Express® που έχουν εκτεθεί σε κίνδυνο.



### Βήμα 4:

Συνεργαστείτε μαζί μας για την επίλυση τυχόν ζητημάτων που απορρέουν από το Περιστατικό Παραβίασης Δεδομένων.

Ανατρέξτε στην [Ενότητα 3, «Υποχρεώσεις διαχείρισης Περιστατικών Παραβίασης Δεδομένων»](#) για περισσότερες πληροφορίες σχετικά με τις Υποχρεώσεις διαχείρισης Περιστατικών Παραβίασης Δεδομένων.

Έχετε και άλλες ερωτήσεις;

ΗΠΑ: (888) 732-3750 (χωρίς χρέωση)

Διεθνείς κλήσεις: +1 (602) 537-3021

[EIRP@aexp.com](mailto:EIRP@aexp.com)

## Ως ηγέτης στην προστασία των καταναλωτών, η American Express έχει μακροχρόνια δέσμευση στην προστασία των Στοιχείων Κατόχου Κάρτας και των Ευαίσθητων Δεδομένων Αυθεντικοποίησης, φροντίζοντας να παραμένουν ασφαλή.

Δεδομένα που έχουν εκτεθεί σε κίνδυνο επηρεάζουν αρνητικά καταναλωτές, Εμπόρους, Παρόχους Υπηρεσιών και εκδότες καρτών. Ακόμη κι ένα περιστατικό μπορεί να βλάψει σοβαρά τη φήμη της εταιρείας και να επηρεάσει την ικανότητά της να διεξάγει αποτελεσματικά τις εργασίες της. Η αντιμετώπιση αυτής της απειλής από την εφαρμογή των πολιτικών λειτουργίας ασφάλειας μπορεί να συμβάλει στη βελτίωση της εμπιστοσύνης των πελατών, την αύξηση της αποδοτικότητας και την ενίσχυση της φήμης μιας εταιρείας.

Στην American Express γνωρίζουν ότι οι Έμποροι και οι Πάροχοι Υπηρεσιών μας (εφεξής συλλογικά **εσείς**) μοιράζονται την ανησυχία μας και ζητούμε, στο πλαίσιο των αρμοδιοτήτων σας, να συμμορφώνεστε με τις διατάξεις ασφάλειας των δεδομένων που περιλαμβάνονται στη συμφωνία σας να δέχεστε (στην περίπτωση των Εμπόρων) ή να επεξεργάζεστε (στην περίπτωση των Παρόχων Υπηρεσιών) την κάρτα American Express® (εκάστη, αντιστοίχως, η **Συμφωνία**) καθώς και αυτήν την Πολιτική Λειτουργίας Ασφάλειας Δεδομένων, την οποία θα ενδέχεται να τροποποιούμε κατά διαστήματα. Αυτές οι προϋποθέσεις ισχύουν για όλο τον εξοπλισμό, τα συστήματα και τα δίκτυά σας (και τα εξαρτήματά τους), στα οποία αποθηκεύονται, υποβάλλονται σε επεξεργασία ή μεταδίδονται τα κλειδιά κρυπτογράφησης, τα Στοιχεία Κατόχου Κάρτας ή τα Ευαίσθητα Δεδομένα Αυθεντικοποίησης (ή συνδυασμός αυτών).

*Οι όροι με κεφαλαία που χρησιμοποιούνται αλλά δεν ορίζονται εδώ έχουν τις έννοιες που τους αποδίδονται στο γλωσσάριο στο τέλος αυτής της πολιτικής.*

## Ενότητα 1 Πρόγραμμα Στοχευμένης Ανάλυσης (TAP)

Ενδέχεται να τεθούν σε κίνδυνο δεδομένα κατόχου κάρτας λόγω κενών στην ασφάλεια δεδομένων τα οποία εντοπίζονται στο Περιβάλλον Δεδομένων Κατόχου Κάρτας (CDE).

Ενδεικτικά παραδείγματα διακινδύνευσης Δεδομένων Κατόχου Κάρτας:

- **Κοινό Σημείο Αγοράς (CPP):** Κάτοχοι Κάρτας American Express αναφέρουν Συναλλαγές στους λογαριασμούς των Καρτών τους οι οποίες είναι αποτέλεσμα απάτης και οι οποίες εντοπίζεται και καθορίζεται ότι προέρχονται από αγορές στις Εγκαταστάσεις σας.
- **Εντοπισμός Δεδομένων Κάρτας:** Εντοπισμός Κάρτας American Express και Δεδομένων Κατόχου Κάρτας στο διαδίκτυο τα οποία συνδέονται με συναλλαγές στις εγκαταστάσεις σας.
- **Υποψία για κακόβουλο λογισμικό:** Η American Express υποψιάζεται ότι χρησιμοποιείτε λογισμικό το οποίο είναι μολυσμένο ή εύαλωτο σε κακόβουλο κώδικα.

Το TAP έχει σχεδιαστεί για να εντοπίζει πιθανές διακινδυνεύσεις δεδομένων Κατόχου Κάρτας.

Πρέπει εσείς οι ίδιοι, αλλά και τα Συμβαλλόμενα Μέρη που Καλύπτονται, να συμμορφώνεστε με τις ακόλουθες απαιτήσεις αμέσως μετά τη λήψη ειδοποίησης από την American Express σχετικά με μια πιθανή διακινδύνευση δεδομένων Κατόχου Κάρτας.

- Πρέπει να ελέγξετε εγκαίρως το CDE σας για κενά σε θέματα ασφάλειας δεδομένων και να διευθετήσετε τυχόν ευρήματα.
  - Πρέπει να ζητήσετε από τυχόν τρίτους προμηθευτές σας να διεξαγάγουν μια λεπτομερή έρευνα του CDE σας, εάν τελεί υπό τη διαχείριση τρίτης εταιρείας.
- Πρέπει να παρέχετε μια περίληψη των ενεργειών που έχουν αναληφθεί ή προγραμματιστεί μετά τις προσπάθειες ανασκόπησης, αξιολόγησης ή/και αντιμετώπισης κατόπιν ειδοποίησης από την American Express.
- Πρέπει να παρέχετε επικαιροποιημένα έγγραφα PCI DSS σύμφωνα με την [Ενότητα 5, «Σημαντική περιοδική επικύρωση των συστημάτων σας»](#).
- Κατά περίπτωση, πρέπει να διορίσετε έναν πιστοποιημένο Εγκληματολογικό Ερευνητή PCI (PCI Forensic Investigator, PFI) για να εξετάσει το CDE σας εάν εσείς ή το Συμβαλλόμενο Μέρος που Καλύπτεται:
  - Δεν είστε σε θέση να επιλύσετε τη διακινδύνευση Δεδομένων Κατόχου Κάρτας εντός εύλογου χρονικού διαστήματος, όπως καθορίζεται από την American Express ή
  - Επιβεβαιώσετε ότι έχει προκύψει Περιστατικό Παραβίασης Δεδομένων και ότι συμμορφώνεστε με τις απαιτήσεις που ορίζονται στην [Ενότητα 3, «Υποχρεώσεις διαχείρισης Περιστατικών Παραβίασης Δεδομένων»](#).

Πίνακας A-1: Τέλος Μη Συμμόρφωσης με το TAP

Περιγραφή	Έμπορος Επιπέδου 1 ή Πάροχος Υπηρεσιών Επιπέδου 1	Έμπορος Επιπέδου 2 ή Πάροχος Υπηρεσιών Επιπέδου 2	Έμπορος Επιπέδου 3 ή Επιπέδου 4
Το τέλος μη συμμόρφωσης ενδέχεται να αξιολογηθεί όταν δεν ικανοποιούνται οι υποχρεώσεις του TAP εντός της πρώτης προθεσμίας.	25.000 \$ (USD)	5.000 \$ (USD)	1.000 \$ (USD)
Το τέλος μη συμμόρφωσης ενδέχεται να αξιολογηθεί όταν δεν ικανοποιούνται οι υποχρεώσεις του TAP έως τη δεύτερη προθεσμία.	35.000 \$ (USD)	10.000 \$ (USD)	2.500 \$ (USD)
Το τέλος μη συμμόρφωσης ενδέχεται να αξιολογηθεί όταν δεν ικανοποιούνται οι υποχρεώσεις του TAP έως την τρίτη προθεσμία. <b>ΣΗΜΕΙΩΣΗ:</b> Τα τέλη μη συμμόρφωσης ενδέχεται να συνεχίσουν να χρεώνονται έως ότου ικανοποιηθούν οι υποχρεώσεις ή αποκατασταθεί το TAP.	45.000 \$ (USD)	15.000 \$ (USD)	5.000 \$ (USD)

Εάν δεν ανταποκριθείτε στις υποχρεώσεις σας στο πλαίσιο του TAP, τότε η American Express έχει το δικαίωμα να επιβάλει σωρευτικά τέλη μη συμμόρφωσης, να αναβάλει πληρωμές ή/και να τερματίσει τη Συμφωνία.

## Ενότητα 2

### Πρότυπα για την προστασία των κλειδιών κρυπτογράφησης, των Στοιχείων Κατόχου Κάρτας και των Ευαίσθητων Δεδομένων Αυθεντικοποίησης

Πρέπει εσείς οι ίδιοι, αλλά και τα Συμβαλλόμενα Μέρη που Καλύπτονται:

- Να αποθηκεύετε Στοιχεία Κατόχου Κάρτας μόνο για τη διευκόλυνση των Συναλλαγών με Κάρτες American Express σύμφωνα με τη Συμφωνία και όπως απαιτείται από αυτήν.
- Να συμμορφώνεστε με τις τρέχουσες απαιτήσεις του PCI DSS και άλλων PCI SSC που ισχύουν σε ό,τι αφορά την επεξεργασία, την αποθήκευση ή τη μετάδοση Στοιχείων Κατόχου Κάρτας ή Ευαίσθητων Δεδομένων Αυθεντικοποίησης το αργότερο έως την ημερομηνία έναρξης ισχύος για την εφαρμογή αυτής της έκδοσης της ισχύουσας απαίτησης.
- Να χρησιμοποιείτε, κατά την ανάπτυξη νέων ή την αντικατάσταση Συσκευών Εισαγωγής PIN ή Εφαρμογών Πληρωμών (ή και των δύο), αποκλειστικά στις περιπτώσεις που είναι εγκεκριμένες από την PCI.

Πρέπει να προστατεύετε όλα τα αρχεία χρεώσεων της American Express και τα πιστωτικά αρχεία που διατηρούνται βάσει της Συμφωνίας, σύμφωνα με αυτές τις διατάξεις ασφάλειας δεδομένων. Πρέπει να χρησιμοποιείτε αυτά τα αρχεία μόνο για τους σκοπούς της Συμφωνίας και να τα διαφυλάσσετε ανάλογα. Είστε οικονομικά και αλλιώς υπόχρεοι απέναντι στην American Express για την εξασφάλιση της συμμόρφωσης των Συμβαλλομένων Μερών που Καλύπτονται με αυτές τις διατάξεις ασφάλειας δεδομένων (πέραν από την απόδειξη της συμμόρφωσης των Συμβαλλομένων Μερών που Καλύπτονται με την παρούσα Πολιτική, σύμφωνα με την [Ενότητα 5, «Σημαντική περιοδική επικύρωση των συστημάτων σας»](#), εκτός εάν προβλέπεται διαφορετικά σε αυτή την ενότητα).

### Ενότητα 3 Υποχρεώσεις διαχείρισης Περιστατικών Παραβίασης Δεδομένων

Πρέπει να ενημερώνετε αμέσως την American Express και σε καμία περίπτωση αργότερα από εβδομήντα δύο (72) ώρες μετά από την ανακάλυψη ενός Περιστατικού Παραβίασης Δεδομένων.

Προκειμένου να ενημερώσετε την American Express, επικοινωνήστε με το Πρόγραμμα Ανταπόκρισης σε Περιστατικά της Επιχείρησης American Express (American Express Enterprise Incident Response Programme, *EIRP*) στο +1 (602) 537-3021 [το + υποδηλώνει το πρόθεμα για διεθνείς άμεσες κλήσεις (IDD), για τις οποίες ισχύουν τέλη διεθνών κλήσεων] ή αποστέλλετε email στη διεύθυνση [EIRP@aexp.com](mailto:EIRP@aexp.com). Πρέπει να ορίσετε ένα άτομο ως επαφή σας σχετικά με ένα τέτοιο Περιστατικό Παραβίασης Δεδομένων. Επιπλέον:

- Πρέπει να διεξάγετε λεπτομερή εγκληματολογική έρευνα για κάθε Περιστατικό Παραβίασης Δεδομένων.
- Για Περιστατικά Παραβίασης Δεδομένων που αφορούν 10.000 ή περισσότερους μοναδικούς Αριθμούς Καρτών, αυτή η έρευνα πρέπει να διεξαχθεί από έναν Εγκληματολογικό Ερευνητή Καρτών Πληρωμής PCI (PFI) εντός πέντε (5) ημερών από τη στιγμή που ανακαλύφθηκε το Περιστατικό Παραβίασης Δεδομένων.
- Η μη επεξεργασμένη αναφορά πρέπει να παρέχεται στην American Express εντός δέκα (10) εργάσιμων ημερών μετά την ολοκλήρωσή της.
- Πρέπει να δώσετε άμεσα στην American Express όλους τους Αριθμούς Καρτών που έχουν εκτεθεί σε κίνδυνο. Η American Express διατηρεί το δικαίωμα να διεξάγει τη δική της εσωτερική ανάλυση προκειμένου να εντοπίσει τους αριθμούς καρτών που σχετίζονται με το Περιστατικό Παραβίασης Δεδομένων.

Οι αναφορές της εγκληματολογικής έρευνας πρέπει να συμπληρώνονται με χρήση του τρέχοντος Υποδείγματος Τελικής Αναφοράς Εγκληματολογικού Συμβάντος που διατίθεται από την PCI. Οι αναφορές εγκληματολογικής έρευνας πρέπει να περιλαμβάνουν εγκληματολογικές εξετάσεις, αναφορές συμμόρφωσης, καθώς και όλες τις άλλες πληροφορίες που σχετίζονται με το Περιστατικό Παραβίασης Δεδομένων, εντοπισμό της αιτίας του Περιστατικού Παραβίασης Δεδομένων, επιβεβαίωση του κατά πόσον είχατε συμμορφωθεί με το PCI DSS κατά τον χρόνο του Περιστατικού Παραβίασης Δεδομένων, και επαλήθευση της ικανότητάς σας να προλαμβάνετε μελλοντικά Περιστατικά Παραβίασης Δεδομένων μέσω της (i) παροχής ενός σχεδίου για την αποκατάσταση όλων των ελλείψεων του PCI DSS και (ii) της συμμετοχής σε πρόγραμμα συμμόρφωσης της American Express (όπως περιγράφεται παρακάτω). Κατόπιν απαίτησης της American Express, θα παράσχετε επικύρωση από έναν Εγκεκριμένο Εκτιμητή Ασφαλείας (Qualified Security Assessor, QSA) ότι οι ελλείψεις έχουν αποκατασταθεί.

Με την επιφύλαξη των προηγούμενων παραγράφων της [Ενότητας 3. «Υποχρεώσεις διαχείρισης Περιστατικών Παραβίασης Δεδομένων»](#):

- Η American Express δύναται, κατά την απόλυτη διακριτική της ευχέρεια, να ζητήσει από εσάς να ορίσετε έναν PFI για τη διενέργεια έρευνας σχετικά με Περιστατικό Παραβίασης Δεδομένων για Περιστατικά Παραβίασης Δεδομένων τα οποία περιλαμβάνουν λιγότερους από 10.000 μοναδικούς αριθμούς καρτών. Κάθε τέτοια έρευνα πρέπει να συμμορφώνεται με τις απαιτήσεις που ορίζονται παραπάνω στην [Ενότητα 3. «Υποχρεώσεις διαχείρισης Περιστατικών Παραβίασης Δεδομένων»](#) και πρέπει να ολοκληρώνεται εντός του χρονικού πλαισίου που απαιτείται από την American Express.
- Η American Express δύναται, κατά την απόλυτη διακριτική της ευχέρεια, να ορίσει ξεχωριστά PFI για τη διενέργεια έρευνας για τυχόν Περιστατικό Παραβίασης Δεδομένων και ενδέχεται να χρεώσει το κόστος μιας τέτοιας έρευνας σε εσάς.

Δέχστε να συνεργαστείτε με την American Express για τη διόρθωση οποιωνδήποτε θεμάτων που εγείρονται από το Περιστατικό Παραβίασης Δεδομένων, μεταξύ άλλων μέσω διαβούλευσης με την American Express σχετικά με την επικοινωνία σας με κατόχους καρτών που επηρεάστηκαν από το Περιστατικό Παραβίασης Δεδομένων και μέσω παροχής (και λήψης τυχόν δηλώσεων αποποίησης ευθύνης που είναι απαραίτητες) στην American Express όλων των σχετικών πληροφοριών για την επαλήθευση της ικανότητάς σας να προλάβετε Περιστατικά Παραβίασης Δεδομένων στο μέλλον κατά τρόπο ο οποίος συνάδει με τη Συμφωνία.

Με την επιφύλαξη τυχόν αντίθετης υποχρέωσης εχεμύθειας της Συμφωνίας, η American Express έχει το δικαίωμα να αποκαλύψει πληροφορίες σχετικά με οποιοδήποτε Περιστατικό Παραβίασης Δεδομένων σε μέλη, εκδότες, άλλους συμμετέχοντες στο δίκτυο American Express και το ευρύ κοινό όπως απαιτείται από την ισχύουσα νομοθεσία. Με δικαστική, διοικητική ή κανονιστική διάταξη, διάταγμα, κλήτευση, αίτημα ή άλλη διαδικασία. Προκειμένου να μετριαστεί ο κίνδυνος απάτης ή άλλης βλάβης, ή άλλως στον βαθμό που απαιτείται για τη λειτουργία του δικτύου American Express.

## Ενότητα 4 Υποχρεώσεις αποζημίωσης για ένα Περιστατικό Παραβίασης Δεδομένων

Οι υποχρεώσεις αποζημίωσής σας προς την American Express βάσει της Συμφωνίας για Περιστατικά Παραβίασης Δεδομένων θα καθοριστούν, χωρίς να υπάρξει παραίτηση από οποιαδήποτε άλλα δικαιώματα και τρόπους αντιμετώπισης εκ μέρους της American Express σύμφωνα με την παρούσα [Ενότητα 4, «Υποχρεώσεις αποζημίωσης για ένα Περιστατικό Παραβίασης Δεδομένων»](#). Επιπρόσθετα στις υποχρεώσεις αποζημίωσης (εφόσον υπάρχουν), ενδέχεται να σας επιβληθεί τέλος μη συμμόρφωσης για Περιστατικά Παραβίασης Δεδομένων, όπως περιγράφεται παρακάτω στην παρούσα [Ενότητα 4, «Υποχρεώσεις αποζημίωσης για ένα Περιστατικό Παραβίασης Δεδομένων»](#).

Για Περιστατικά Παραβίασης Δεδομένων που περιλαμβάνουν:

- 10.000 και άνω Αριθμούς Καρτών American Express με ένα από τα ακόλουθα:
  - Ευαίσθητα Δεδομένα Αυθεντικοποίησης ή
  - Ημερομηνία λήξης

Θα αποζημιώσετε την American Express με ποσό 5 \$ (USD) ανά αριθμό λογαριασμού.

Ωστόσο, η American Express δεν θα ζητήσει αποζημίωση από εσάς για ένα Περιστατικό Παραβίασης Δεδομένων το οποίο περιλαμβάνει:

- Λιγότερους από 10.000 μοναδικούς Αριθμούς Κάρτας American Express ή
- Περισσότερους από 10.000 Αριθμούς Κάρτας American Express, εάν πληροίτε τις ακόλουθες συνθήκες:
  - ενημερώσατε την American Express για το Περιστατικό Παραβίασης Δεδομένων σύμφωνα με την [Ενότητα 3, «Υποχρεώσεις διαχείρισης Περιστατικών Παραβίασης Δεδομένων»](#),
  - συμμορφώσασταν κατά τη στιγμή του Περιστατικού Παραβίασης Δεδομένων με το PCI DSS (όπως καθορίστηκε από την έρευνα του PFI για το Περιστατικό Παραβίασης Δεδομένων) και
  - το Περιστατικό Παραβίασης Δεδομένων δεν προκλήθηκε από δική σας παράνομη συμπεριφορά ή από την συμπεριφορά των Συμβαλλομένων Μερών σας που Καλύπτονται.

Με την επιφύλαξη των προηγούμενων παραγράφων της [Ενότητας 4, «Υποχρεώσεις αποζημίωσης για ένα Περιστατικό Παραβίασης Δεδομένων»](#), για κάθε Περιστατικό Παραβίασης Δεδομένων, ανεξάρτητα από τον αριθμό των Αριθμών Κάρτας American Express, πρέπει να καταβάλλετε στην American Express ένα τέλος μη συμμόρφωσης για Περιστατικά Παραβίασης Δεδομένων το οποίο δεν θα υπερβαίνει τα 100.000 \$ (USD) ανά Περιστατικό Παραβίασης Δεδομένων (όπως καθορίστηκε από την American Express κατά την απόλυτη διακριτική της ευχέρεια) σε περίπτωση που δεν καταφέρετε να συμμορφωθείτε με οποιαδήποτε από τις υποχρεώσεις σας που ορίζονται στην [Ενότητα 3, «Υποχρεώσεις διαχείρισης Περιστατικών Παραβίασης Δεδομένων»](#). Προς αποφυγή αμφιβολιών, το συνολικό τέλος μη συμμόρφωσης για Περιστατικά Παραβίασης Δεδομένων δεν θα πρέπει να υπερβαίνει τα 100.000 \$ (USD) για κάθε Περιστατικό Παραβίασης Δεδομένων ξεχωριστά.

Η American Express θα εξαιρεί από τους υπολογισμούς της οποιονδήποτε Αριθμό Λογαριασμού Κάρτας της American Express ο οποίος ενεπλάκη σε προηγούμενη αξίωση αποζημίωσης για Περιστατικό Παραβίασης Δεδομένων η οποία υποβλήθηκε εντός διαστήματος δώδεκα (12) μηνών πριν από την Ημερομηνία Είδοποίησης. Όλοι οι υπολογισμοί που γίνονται από την American Express με χρήση αυτής της μεθοδολογίας είναι οριστικοί.

Η American Express ενδέχεται να σας χρεώσει το συνολικό ποσό των υποχρεώσεων αποζημίωσης για Περιστατικά Παραβίασης Δεδομένων ή να αφαιρέσει το ποσό από τις πληρωμές της American Express προς εσάς (ή να χρεώσει κατάλληλα τον Τραπεζικό σας Λογαριασμό) σύμφωνα με την παρούσα Συμφωνία.

Οι υποχρεώσεις αποζημίωσης για τα Περιστατικά Παραβίασης Δεδομένων σύμφωνα με την παρούσα δεν θα θεωρούνται τυχαίες, έμμεσες, κερδοσκοπικές, επακόλουθες, ειδικές, τιμωρητικές ή υποδειγματικές ζημιές στο πλαίσιο της Συμφωνίας, με την προϋπόθεση ότι οι υποχρεώσεις αυτές δεν περιλαμβάνουν ζημιές που σχετίζονται ή έχουν ως αποτέλεσμα απώλεια κερδών ή εσόδων, απώλεια υπεραξίας ή απώλεια επιχειρηματικών ευκαιριών.

Κατά την απόλυτη κρίση της, η American Express μπορεί να μειώσει την υποχρέωση αποζημίωσης για τους Εμπόρους αποκλειστικά για Περιστατικά Παραβίασης Δεδομένων που πληρούν όλα τα παρακάτω κριτήρια:

- Οι εφαρμοζόμενες τεχνολογίες για τον περιορισμό των κινδύνων χρησιμοποιήθηκαν πριν από το Περιστατικό Παραβίασης Δεδομένων και χρησιμοποιήθηκαν κατά τη διάρκεια ολόκληρου του Παραθύρου Συμβάντος του Περιστατικού Παραβίασης Δεδομένων,
- Έχει ολοκληρωθεί μια ενδεδειγμένη έρευνα σύμφωνα με το πρόγραμμα Εγκληματολογικής Έρευνας της Βιομηχανίας Καρτών Πληρωμής (PFI) (εκτός αν έχει προηγουμένως συμφωνηθεί διαφορετικά και εγγράφως),

- Η εγκληματολογική αναφορά αναφέρει σαφώς τις Τεχνολογίες Μετρίασης Κινδύνων που χρησιμοποιήθηκαν για την επεξεργασία, αποθήκευση ή/και μετάδοση των δεδομένων κατά τον χρόνο του Περιστατικού Παραβίασης Δεδομένων, και
- Δεν αποθηκεύετε (και δεν είχατε αποθηκεύσει κατά τη διάρκεια του Παραθύρου Συμβάντος του Περιστατικού Παραβίασης Δεδομένων) Ευαίσθητα Δεδομένα Αυθεντικοποίησης ή οποιαδήποτε Στοιχεία Κατόχου Κάρτας τα οποία δεν κατέστησαν μη αναγνώσιμα.

Όταν υπάρχει μείωση της αποζημίωσης, η μείωση της υποχρέωσής σας περί αποζημίωσης (εξαιρουμένων των πληρωτέων τελών μη συμμόρφωσης) καθορίζεται ως εξής:

**Πίνακας A-2: Απαιτούμενα Κριτήρια για Μείωση των Υποχρεώσεων Αποζημίωσης**

Μείωση Υποχρεώσεων Αποζημίωσης	Απαιτούμενα κριτήρια
Τυπική μείωση: 50%	>75% του συνόλου των συναλλαγών που έχουν υποστεί επεξεργασία σε Συσκευές με Δυνατότητα για Τσιπ <sup>1</sup> Η Τεχνολογία Μετρίασης Κινδύνων σε χρήση σε >75% των τοποθεσιών Εμπόρων <sup>2</sup>
Ενισχυμένη Μείωση: 75% έως 100%	>75% όλων των συναλλαγών που υποβάλλονται σε επεξεργασία σε Συσκευές με Δυνατότητα για Τσιπ <sup>1</sup> ΚΑΙ σε άλλη Τεχνολογία Μετρίασης Κινδύνων που χρησιμοποιείται σε >75% των τοποθεσιών Εμπόρων <sup>2</sup>

<sup>1</sup> Όπως προσδιορίζεται από την εσωτερική ανάλυση της American Express

<sup>2</sup> Όπως προσδιορίζεται από την έρευνα PFI

- Η Ενισχυμένη Μείωση (75% έως 100%) καθορίζεται βάσει του χαμηλότερου ποσοστού των Συναλλαγών με τη χρήση Συσκευών με Δυνατότητα για Τσιπ ΚΑΙ βάσει θέσεων Εμπόρων χρησιμοποιώντας άλλη Τεχνολογία Μετρίασης Κινδύνων. Τα παρακάτω παραδείγματα απεικονίζουν τον υπολογισμό μείωσης της αποζημίωσης.
- Για να θεωρηθεί ότι χρησιμοποιείτε Τεχνολογία Μετρίασης Κινδύνων, πρέπει να αποδείξετε την αποτελεσματική χρήση της τεχνολογίας σύμφωνα με τον σχεδιασμό και τον προορισμό της. Για παράδειγμα, η ανάπτυξη Συσκευών με Δυνατότητα για Τσιπ και η επεξεργασία των Καρτών με Τσιπ ως συναλλαγές με Μαγνητική Ταινία ή με Εισαγωγή Κλειδιού ΔΕΝ αποτελεί αποτελεσματική χρήση αυτής της τεχνολογίας.
- Το ποσοστό επί τοις εκατό των τοποθεσιών που χρησιμοποιούν κάποια Τεχνολογία Μετρίασης Κινδύνων καθορίζεται από την έρευνα του PFI.
- Η μείωση της υποχρέωσης αποζημίωσης δεν ισχύει για τυχόν τέλη μη συμμόρφωσης πληρωτέα σε σχέση με το Περιστατικό Παραβίασης Δεδομένων.

**Πίνακας A-3: Ενισχυμένη Μείωση Υποχρεωτικής Αποζημίωσης**

Π.χ.	Τεχνολογίες Περιορισμού του Κινδύνου που χρησιμοποιούνται	Πληροί τις Προϋποθέσεις	Μείωση
1	80% του Συνόλου των Συναλλαγών που Έχουν Υποστεί Επεξεργασία σε Συσκευές με Δυνατότητα για Τσιπ	Όχι	50%: Τυπική Μείωση (χρήση χαμηλότερη από 75% Τεχνολογίας Μετρίασης Κινδύνων δεν πληροί τις προϋποθέσεις για Ενισχυμένη Μείωση) <sup>1</sup>
	0% των τοποθεσιών χρησιμοποιούν άλλη Τεχνολογία Μετρίασης Κινδύνων		

Π.χ.	Τεχνολογίες Περιορισμού του Κινδύνου που χρησιμοποιούνται	Πληροί τις Προϋποθέσεις	Μείωση
2	80% του Συνόλου των Συναλλαγών που Έχουν Υποστεί Επεξεργασία σε Συσκευές με Δυνατότητα για Τσιπ	Ναι	77%: Ενισχυμένη μείωση (βασισμένη σε χρήση 77% Τεχνολογίας Μετρίασης Κινδύνων)
	77% των τοποθεσιών χρησιμοποιούν άλλη Τεχνολογία Μετρίασης Κινδύνων		
3	93% του Συνόλου των Συναλλαγών που Έχουν Υποστεί Επεξεργασία σε Συσκευές με Δυνατότητα για Τσιπ	Ναι	93%: Ενισχυμένη μείωση (βάσει του 93% του συνόλου των Συναλλαγών σε Συσκευές με Δυνατότητα για Τσιπ)
	100% των τοποθεσιών χρησιμοποιούν άλλη Τεχνολογία Μετρίασης Κινδύνων		
4	40% του Συνόλου των Συναλλαγών που Έχουν Υποστεί Επεξεργασία σε Συσκευές με Δυνατότητα για Τσιπ	Όχι	50%: Τυπική Μείωση (λιγότερο από 75% των Συναλλαγών σε Συσκευές με Δυνατότητα για Τσιπ δεν πληρούν τις προϋποθέσεις για Ενισχυμένη Μείωση)
	90% των τοποθεσιών χρησιμοποιούν άλλη Τεχνολογία Μετρίασης Κινδύνων		

<sup>1</sup> Ένα Περιστατικό Παραβίασης Δεδομένων που περιλαμβάνει 10.000 αριθμούς καρτών American Express με τιμή 5 \$ (USD) ανά αριθμό λογαριασμού (10.000 x 5 \$ = 50.000 \$ [USD]) μπορεί να είναι επιλέξιμο για μείωση κατά 50%, μειώνοντας τις Υποχρεώσεις Αποζημίωσης από 50.000 \$ σε 25.000 \$ (USD), εξαιρουμένων οποιωνδήποτε τελών μη συμμόρφωσης.

## Ενότητα 5

### Σημαντική περιοδική επικύρωση των συστημάτων σας

Πρέπει να ακολουθήσετε τα παρακάτω βήματα για να επικυρώσετε στο PCI DSS ετησίως και κάθε 90 ημέρες, όπως περιγράφεται κατωτέρω, την κατάσταση του εξοπλισμού, των συστημάτων ή/και των δικτύων (και των εξαρτημάτων τους) από τους Δικαιοδόχους σας, στα οποία αποθηκεύονται, υποβάλλονται σε επεξεργασία ή μεταδίδονται Στοιχεία Κατόχου Κάρτας ή Ευαίσθητα Δεδομένα Αυθεντικοποίησης.

Για την ολοκλήρωση της επικύρωσης απαιτούνται τέσσερα βήματα:

[Βήμα 1:](#) Εγγραφείτε στο πρόγραμμα συμμόρφωσης PCI της American Express («το Πρόγραμμα») βάσει της παρούσας πολιτικής.

[Βήμα 2:](#) Προσδιορίστε το Επίπεδο Εμπόρου στο οποίο υπάγεστε και τις Απαιτήσεις Επικύρωσης.

[Βήμα 3:](#) Προσδιορίστε την Τεκμηρίωση Επικύρωσης που πρέπει να στείλετε στην American Express.

[Βήμα 4:](#) Στείλτε την Τεκμηρίωση Επικύρωσης στην American Express εντός των προβλεπόμενων χρονοδιαγραμμάτων.

### Βήμα 1: Εγγραφείτε στο Πρόγραμμα Συμμόρφωσης της American Express στο πλαίσιο αυτής της Πολιτικής

Οι Έμποροι Επιπέδου 1, οι Έμποροι Επιπέδου 2 και όλοι οι Πάροχοι Υπηρεσιών, όπως περιγράφεται κατωτέρω, πρέπει να συμμετάσχουν στο Πρόγραμμα βάσει της παρούσας πολιτικής. Η American Express πρέπει να ορίσει, κατά την απόλυτη διακριτική της ευχέρεια, ειδικούς Εμπόρους Επιπέδου 3 και Επιπέδου 4 για να συμμετάσχουν στο Πρόγραμμα βάσει της παρούσας πολιτικής.

Οι Έμποροι και οι Πάροχοι Υπηρεσιών που απαιτούνται για τη συμμετοχή στο Πρόγραμμα πρέπει να εγγραφούν στην Πύλη η οποία παρέχεται από τον Διαχειριστή Προγράμματος που επιλέγεται από την American Express εντός των προβλεπόμενων χρονοδιαγραμμάτων.



- Πρέπει να αποδεχθείτε όλους τους εύλογους όρους και προϋποθέσεις που συνδέονται με τη χρήση της Πύλης.
- Πρέπει να εκχωρείτε και να παρέχετε ακριβείς πληροφορίες για τουλάχιστον ένα άτομο επικοινωνίας σε θέματα ασφάλειας δεδομένων εντός της Πύλης. Τα απαιτούμενα στοιχεία δεδομένων περιλαμβάνουν τα εξής:
  - ονοματεπώνυμο
  - διεύθυνση email
  - αριθμό τηλεφώνου
  - ταχυδρομική διεύθυνση
- Πρέπει να παρέχετε επικαιροποιημένα ή νέα στοιχεία επικοινωνίας του ατόμου που είναι υπεύθυνο για την ασφάλεια των δεδομένων εντός της Πύλης κάθε φορά που αλλάζουν.
- Πρέπει να διασφαλίζετε ότι τα συστήματά σας είναι επικαιροποιημένα, ώστε να επιτρέπονται οι επικοινωνίες σχετικά με την παροχή υπηρεσιών από τον καθορισμένο τομέα της Πύλης.

Η αδυναμία παροχής ή διατήρησης επικαιροποιημένων στοιχείων επικοινωνίας με το άτομο που είναι υπεύθυνο για την ασφάλεια δεδομένων ή παροχής της δυνατότητας επικοινωνίας μέσω email δεν θα επηρεάσει τα δικαιώματά σας να αξιολογήσετε τα τέλη.

## Βήμα 2: Προσδιορίστε το Επίπεδο Εμπόρου στο οποίο υπάγεστε και τις Απαιτήσεις Επικύρωσης

Υπάρχουν τέσσερα Επίπεδα Εμπόρου για τους Εμπόρους και δύο Επίπεδα για τους Παρόχους Υπηρεσιών, τα οποία βασίζονται στον όγκο των συναλλαγών καρτών American Express.

- Για τους Εμπόρους, αυτός είναι ο όγκος που υποβάλλεται από τις Εγκαταστάσεις τους που εκτείνονται έως το υψηλότερο επίπεδο λογαριασμού Εμπόρων της American Express.\*
- Για τους Παρόχους Υπηρεσιών, αυτό είναι το σύνολο του όγκου που υποβάλλεται από τον Πάροχο Υπηρεσιών και τον Πάροχο Υπηρεσιών Οντοτήτων στον οποίο παρέχετε τις υπηρεσίες.

Πληρωμές με Πρωτοβουλία Επιχειρήσεων (Buyer Initiated Payments, BIP) δεν συμπεριλαμβάνονται στον όγκο των Συναλλαγών Καρτών American Express για καθορισμό του Επιπέδου Εμπορικών Συναλλαγών και Απαιτήσεων Επικύρωσης. Θα υπάγεστε σε ένα από τα Επίπεδα Εμπόρου που καθορίζονται στους παρακάτω πίνακες Εμπόρων και Παρόχων Υπηρεσιών.

\* Στην περίπτωση των δικαιοπαρόχων, αυτό περιλαμβάνει τον όγκο των Εγκαταστάσεων του δικαιοδόχου. Οι δικαιοπάροχοι που εξουσιοδοτούν τους δικαιοδόχους να χρησιμοποιούν ένα συγκεκριμένο Σύστημα Πώλησης (Point of Sale, POS) ή Πάροχο Υπηρεσιών πρέπει επίσης να παρέχουν τεκμηρίωση επικύρωσης για τους επηρεαζόμενους Δικαιοδόχους.

## Απαιτήσεις Τεκμηρίωσης Επικύρωσης Εμπόρων

Οι Έμποροι (όχι Πάροχοι Υπηρεσιών) έχουν τέσσερις δυνατές ταξινομήσεις Επιπέδου Εμπόρου. Αφού καθοριστεί το επίπεδο του Εμπόρου από τον παρακάτω κατάλογο, βλ. [Πίνακας A-4: Τεκμηρίωση Επικύρωσης Εμπόρου](#) για καθορισμό των απαιτήσεων τεκμηρίωσης επικύρωσης.

- **Έμπορος Επιπέδου 1** – 2,5 εκατομμύρια Συναλλαγές Κάρτας American Express ή περισσότερες ανά έτος· ή οποιοσδήποτε Έμπορος που η American Express κρίνει ότι εντάσσεται στο Επίπεδο 1.
- **Έμπορος Επιπέδου 2** – 50.000 έως 2,5 εκατομμύρια Συναλλαγές Κάρτας American Express ανά έτος.
- **Έμπορος Επιπέδου 3** – 10.000 έως 50.000 Συναλλαγές Κάρτας American Express ανά έτος.
- **Έμπορος Επιπέδου 4** – Κάτω από 10.000 Συναλλαγές Κάρτας American Express ανά έτος.

**Πίνακας A-4: Τεκμηρίωση Επικύρωσης Εμπόρου**

Επίπεδο Εμπόρου/ Ετήσιες συναλλαγές American Express	Έκθεση σε Θέματα Συμμόρφωσης με τίτλο Βεβαίωση Συμμόρφωσης (ROC AOC)	Ερωτηματολόγιο σχετικά με τη Βεβαίωση Συμμόρφωσης (SAQ AOC) ΚΑΙ Τριμηνιαία Σάρωση Τρωτών Σημείων Εξωτερικού Δικτύου (Σάρωση)	Πιστοποίηση STEP για επιλέξιμους Εμπόρους
Επίπεδο 1/ 2,5 εκατομμύρια και άνω	Υποχρεωτική	Δεν ισχύει	Προαιρετική με την έγκριση της American Express (αντικαθιστά τη ROC)
Επίπεδο 2/ 50.000 έως 2,5 εκατομμύρια	Προαιρετική	Υποχρεωτικό SAQ AOC (εκτός εάν γίνεται υποβολή ROC AOC)- υποχρεωτική σάρωση με συγκεκριμένους τύπους SAQ	Προαιρετική (αντικαθιστά το SAQ και τη σάρωση δικτύου ή τη ROC)
Επίπεδο 3/ 10.000 έως 50.000	Προαιρετική	Προαιρετικό SAQ AOC (υποχρεωτικό εάν απαιτείται από την American Express)- υποχρεωτική σάρωση με συγκεκριμένους τύπου SAQ	Προαιρετική (αντικαθιστά το SAQ και τη σάρωση δικτύου ή τη ROC)
Επίπεδο 4/ 10.000 και κάτω	Προαιρετική	Προαιρετικό SAQ AOC (υποχρεωτικό εάν απαιτείται από την American Express)- υποχρεωτική σάρωση με συγκεκριμένους τύπου SAQ	Προαιρετική (αντικαθιστά το SAQ και τη σάρωση δικτύου ή τη ROC)

\* Για την αποφυγή αμφιβολιών, οι Έμποροι Επιπέδων 3 και 4 δεν χρειάζεται να υποβάλλουν Τεκμηρίωση Επικύρωσης, εκτός εάν απαιτείται σύμφωνα με τη διακριτική ευχέρεια της American Express, αλλά πρέπει να συμμορφώνονται με όλες τις άλλες διατάξεις της παρούσας Πολιτικής Λειτουργίας Ασφάλειας Δεδομένων και είναι υπόλογοι βάσει αυτής.

Η American Express διατηρεί το δικαίωμα να επαληθεύσει την πληρότητα, την ακρίβεια και την καταλληλότητα της Τεκμηρίωσης Επικύρωσης PCI που διατηρείτε. Η American Express μπορεί να ζητήσει την προσκόμιση πρόσθετων υποστηρικτικών εγγράφων προς αξιολόγηση για αυτόν τον σκοπό. Επιπλέον, η American Express διατηρεί το δικαίωμα να ζητήσει τη συμμετοχή σας σε ένα PCI Security Standards Council το οποίο είναι εγκεκριμένο από QSA ή PFI.

### Πρόγραμμα Ενίσχυσης Τεχνολογίας Ασφάλειας (STEP)

Οι Έμποροι που συμμορφώνονται με το PCI DSS μπορούν, κατά την κρίση της American Express, να πληρούν τις προϋποθέσεις για το πρόγραμμα STEP (Security Technology Enhancement Programme) της American Express εάν αναπτύξουν ορισμένες πρόσθετες τεχνολογίες ασφάλειας σε ολόκληρο το περιβάλλον επεξεργασίας καρτών τους. Το STEP ισχύει μόνο εάν δεν έχει σημειωθεί Περιστατικό Παραβίασης Δεδομένων κατά τους προηγούμενους 12 μήνες και αν το 75% όλων των συναλλαγών Καρτών του Εμπόρου εκτελείται με χρήση ενός συνδυασμού των ακόλουθων επιλογών ενισχυμένης ασφάλειας:

- **EMV, Ανέπαφες Συναλλαγές EMV ή Ψηφιακό Πορτοφόλι** – σε μια Συσκευή με Δυνατότητα για Τσιπ που έχει έγκυρη και τρέχουσα έγκριση/πιστοποίηση EMVCo ([www.emvco.com](http://www.emvco.com)) και είναι ικανή για Επεξεργασία Συναλλαγών με Τσιπ που συμμορφώνονται με το AEIPS. (Οι Έμποροι των ΗΠΑ πρέπει να συμπεριλαμβάνουν και Ανέπαφες Συναλλαγές)
- **Δισημειακή Κρυπτογράφηση (P2PE)** – που γνωστοποιήθηκε στον επεξεργαστή του Εμπόρου χρησιμοποιώντας ένα σύστημα Δισημειακής Κρυπτογράφησης εγκεκριμένο από την PCI SSC ή εγκεκριμένο από την QSA
- **Αντικαταστημένο με ψηφιακά τεκμήρια (tokenised)** – η εφαρμοζόμενη λύση δημιουργίας ψηφιακών τεκμηρίων (tokenisation) πρέπει:
  - να πληροί τις προδιαγραφές EMVCo,
  - να είναι ασφαλής, να έχει υποβληθεί σε επεξεργασία, να αποθηκεύεται, να μεταδίδεται και να τελεί εξολοκλήρου υπό τη διαχείριση ενός τρίτου παρόχου υπηρεσιών που συμμορφώνεται με το πρότυπο PCI, ενώ

- δεν μπορεί να γίνει αντιστροφή της κωδικοποίησης του Ψηφιακού Τεκμηρίου (token), προκειμένου να αποκαλυφθούν μη καλυμμένοι Πρωτεύοντες Αριθμοί Λογαριασμού (PAN) στον Έμπορο.

Οι Έμποροι που είναι επιλέξιμοι για το Πρόγραμμα STEP έχουν μειώσει τις προϋποθέσεις τεκμηρίωσης της επικύρωσης PCI, όπως περιγράφεται περαιτέρω στο [Βήμα 3: «Προσδιορίστε την Τεκμηρίωση Επικύρωσης που πρέπει να στείλετε στην American Express»](#) παρακάτω.

### Προϋποθέσεις Παρόχου Υπηρεσιών

Οι Πάροχοι Υπηρεσιών (όχι οι Έμποροι) έχουν δύο πιθανές ταξινομήσεις Επιπέδου. Αφού καθοριστεί το επίπεδο του Παρόχου Υπηρεσιών από τον παρακάτω κατάλογο, βλ. [Πίνακας A-5: Τεκμηρίωση Παρόχου Υπηρεσιών](#) για καθορισμό των απαιτήσεων τεκμηρίωσης επικύρωσης.

**Πάροχος Υπηρεσιών Επιπέδου 1** – 2,5 εκατομμύρια Συναλλαγές Κάρτας American Express ή περισσότερες ανά έτος ή· οποιοσδήποτε Πάροχος Υπηρεσιών που η American Express κρίνει ότι εντάσσεται στο Επίπεδο 1.

**Πάροχος Υπηρεσιών Επιπέδου 2** – λιγότερο από 2,5 εκατομμύρια Συναλλαγές Κάρτας American Express ανά έτος ή· οποιοσδήποτε Πάροχος Υπηρεσιών δεν κρίνεται ως Επίπεδο 1 από την American Express.

Οι Πάροχοι Υπηρεσιών δεν είναι επιλέξιμοι για το πρόγραμμα STEP.

### Πίνακας A-5: Τεκμηρίωση Παρόχου Υπηρεσιών

Επίπεδο	Τεκμηρίωση Επικύρωσης	Προϋπόθεση
1	Ετήσια Έκθεση σε Θέματα Συμμόρφωσης με τίτλο Βεβαίωση Συμμόρφωσης (ROC AOC)	Υποχρεωτική
2	Ετήσιο SAQ D (Πάροχος Υπηρεσιών) και Τριμηνιαία Σάρωση Δικτύου ή Ετήσια Έκθεση σε Θέματα Συμμόρφωσης με τίτλο Βεβαίωση Συμμόρφωσης (ROC AOC), εάν προτιμάται	Υποχρεωτική

Συνιστάται οι Πάροχοι Υπηρεσιών να συμμορφώνονται επίσης με τη Συμπληρωματική Επικύρωση των Καθορισμένων Οντοτήτων PCI.

### Βήμα 3: Προσδιορίστε την Τεκμηρίωση Επικύρωσης που πρέπει να στείλετε στην American Express

Τα παρακάτω έγγραφα απαιτούνται για διαφορετικά επίπεδα Εμπόρων και Παρόχων Υπηρεσιών όπως αναφέρονται στον Πίνακα Εμπόρων και τον Πίνακα Παρόχων Υπηρεσιών παραπάνω.

Πρέπει να παρέχετε Βεβαίωση Συμμόρφωσης (AOC) για τον τύπο αξιολόγησης που εφαρμόζεται. Η AOC είναι μια δήλωση της κατάστασης συμμόρφωσής σας και, ως εκ τούτου, πρέπει να υπογράφεται και να χρονολογείται από άτομο το οποίο κατέχει θέση σε κατάλληλο επίπεδο ηγεσίας εντός του οργανισμού σας.

Επιπρόσθετα στην AOC, η American Express ενδέχεται να ζητήσει από εσάς να παρέχετε ένα αντίγραφο της πλήρους αξιολόγησης και, κατά τη διακριτική σας ευχέρεια, πρόσθετα υποστηρικτικά έγγραφα που επιδεικνύουν συμμόρφωση με τις απαιτήσεις PCI DSS. Η εν λόγω Τεκμηρίωση Επικύρωσης ολοκληρώνεται με δικά σας έξοδα.

**Έκθεση σε Θέματα Συμμόρφωσης με τίτλο Βεβαίωση Συμμόρφωσης (ROC AOC) - (Ετήσια Απαίτηση)** – Η Έκθεση σε θέματα Συμμόρφωσης καταγράφει τα αποτελέσματα μιας λεπτομερούς επιτόπιας εξέτασης του εξοπλισμού, των συστημάτων και των δικτύων σας (και των εξαρτημάτων τους) στα οποία αποθηκεύονται, υποβάλλονται σε επεξεργασία ή μεταδίδονται Στοιχεία Κατόχου Κάρτας ή Ευαίσθητα Δεδομένα Αυθεντικοποίησης. Υπάρχουν δύο εκδόσεις: μία για Εμπόρους και μία άλλη για Παρόχους Υπηρεσιών. Η Έκθεση σε Θέματα Συμμόρφωσης πρέπει να συνταχθεί από:

- έναν QSA ή
- από εσάς και να επικυρώνεται από τον διευθύνοντα σύμβουλό σας, τον οικονομικό διευθυντή, τον επικεφαλής της υπηρεσίας ασφάλειας πληροφοριών ή τον κύριο υπόχρεο.

Η AOC πρέπει να υπογράφεται και να χρονολογείται από έναν QSA ή έναν Εσωτερικό Εκτιμητή Ασφάλειας (ISA) και από ένα άτομο το οποίο κατέχει θέση σε εγκεκριμένο επίπεδο ηγεσίας εντός του οργανισμού σας και να προσκομίζεται στην American Express τουλάχιστον μία φορά ετησίως.

**Ερωτηματολόγιο Αυτοαξιολόγησης ως προς τη Βεβαίωση Συμμόρφωσης (SAQ AOC) - (Ετήσια Απαιτήση)** – Το Ερωτηματολόγιο Αυτοαξιολόγησης παρέχει τη δυνατότητα αυτοεξέτασης του εξοπλισμού, των συστημάτων και των δικτύων σας (και των εξαρτημάτων τους) στα οποία αποθηκεύονται, υποβάλλονται σε επεξεργασία ή μεταδίδονται Στοιχεία Κατόχου Κάρτας ή Ευαίσθητα Δεδομένα Αυθεντικοποίησης. Υπάρχουν πολλές εκδόσεις του SAQ. Θα επιλέξετε μία ή περισσότερες με βάση το Περιβάλλον Δεδομένων Κατόχου Κάρτας.

Το SAQ πρέπει να συμπληρώνεται από προσωπικό εντός της Εταιρείας σας το οποίο είναι πιστοποιημένο να απαντά στις ερωτήσεις με ακρίβεια και διεξοδικά. Εναλλακτικά, μπορείτε να καταφύγετε στη βοήθεια ενός QSA. Η AOC πρέπει να υπογράφεται και να χρονολογείται από άτομο το οποίο κατέχει θέση σε εγκεκριμένο επίπεδο ηγεσίας εντός του οργανισμού σας και να προσκομίζεται στην American Express τουλάχιστον μία φορά ετησίως.

**Περίληψη της Εγκεκριμένης Σάρωσης Τρωτών Σημείων του Εξωτερικού Δικτύου Προμηθευτών (Σάρωση ASV) - (Απαιτήση 90 ημερών)** – Μια εξωτερική σάρωση των τρωτών σημείων είναι ένας εξ αποστάσεως έλεγχος ο οποίος βοηθά στον εντοπισμό δυνητικών αδυναμιών, τρωτών σημείων και εσφαλμένων διαμορφώσεων στοιχείων με πρόσβαση στο Διαδίκτυο τα οποία περιέχει το Περιβάλλον Δεδομένων Κατόχου Κάρτας (π.χ. ιστότοποι, εφαρμογές, διακομιστές web, διακομιστές ηλεκτρονικού ταχυδρομείου, δημόσιοι τομείς ή κεντρικοί υπολογιστές).

Η Σάρωση ASV πρέπει να εκτελείται από έναν Εγκεκριμένο Προμηθευτή Σάρωσης (Approved Scanning Vendor, ASV).

Εάν απαιτείται από το SAQ, η Βεβαίωση Συμμόρφωσης Σάρωσης (AOSC) της Έκθεσης Ελέγχου ASV ή η περίληψη, συμπεριλαμβανομένου ενός αριθμού των στόχων που υποβλήθηκε σε σάρωση, η πιστοποίηση ότι τα αποτελέσματα πληρούν τις διαδικασίες σάρωσης PCI DSS και η κατάσταση συμμόρφωσης που ολοκληρώθηκε από τον ASV, πρέπει να υποβάλλεται στην American Express τουλάχιστον μία φορά κάθε 90 ημέρες.

Δεν απαιτείται να παρέχεται AOSC ή περίληψη της Σάρωσης ASV στο πλαίσιο των ROC AOC ή STEP, εκτός εάν ζητηθεί ειδικά. Για την αποφυγή τυχόν αμφιβολιών, οι Σαρώσεις είναι υποχρεωτικές, εφόσον απαιτείται από το χρησιμοποιούμενο SAQ.

Για την αποφυγή τυχόν αμφιβολιών, η χρήση ASV είναι υποχρεωτική, εφόσον απαιτείται από το χρησιμοποιούμενο SAQ.

**Τεκμηρίωση Επικύρωσης Πιστοποίησης του STEP (STEP) - (Ετήσια Απαιτήση)** – Το STEP διατίθεται μόνο σε Εμπόρους που πληρούν τα κριτήρια τα οποία αναγράφονται στο [Βήμα 2: «Προσδιορίστε το Επίπεδο Εμπόρου στο οποίο υπάγεστε και τις Απαιτήσεις Επικύρωσης»](#) παρακάτω. Εάν η εταιρεία σας πληροί τις προϋποθέσεις, πρέπει να συμπληρώνετε και να υποβάλλετε το έντυπο Πιστοποίησης του STEP ετησίως στην American Express. Το Έντυπο Πιστοποίησης του STEP είναι διαθέσιμο για λήψη από την Πύλη.

**Μη Συμμόρφωση με το PCI DSS - (Απαιτήση Ετήσια, Κάθε 90 Ημέρες ή/και Ad Hoc)** – Εάν δεν συμμορφώνεστε με το PCI DSS, τότε πρέπει να συμπληρώσετε ένα από τα παρακάτω έγγραφα:

- μια Βεβαίωση Συμμόρφωσης (AOC) μαζί με το «Μέρος 4. Σχέδιο Δράσης για Κατάσταση Μη Συμμόρφωσης» (διαθέσιμο για λήψη μέσω του ιστότοπου του PCI Security Standards Council)
- μια Σύνοψη Εργαλείων Προσέγγισης με Ιεράρχηση Προτεραιοτήτων PCI (διαθέσιμο για λήψη μέσω του ιστότοπου του PCI Security Standards Council)
- ένα πρότυπο σχεδίου έργου (διαθέσιμο για λήψη από την Πύλη). Πρέπει να υποβληθεί ένα Σχέδιο Έργου έναντι της ετήσιας πιστοποίησης (SAQ/ROC) ή/και αντί της απαίτησης σάρωσης.

Καθένα από τα παραπάνω έγγραφα πρέπει να αναφέρει μια ημερομηνία αποκατάστασης η οποία δεν πρέπει να υπερβαίνει τους δώδεκα (12) μήνες μετά την ημερομηνία συμπλήρωσης του εγγράφου, για την επίτευξη συμμόρφωσης. Θα πρέπει να παρέχετε στην American Express περιοδικές ενημερώσεις σχετικά με την πρόοδό σας για αποκατάσταση της Κατάστασης Μη Συμμόρφωσης (Εμποροι Επιπέδου 1, Επιπέδου 2, Επιπέδου 3 και Επιπέδου 4, καθώς και όλοι οι Πάροχοι Υπηρεσιών). Τα έξοδα για την εφαρμογή των βημάτων αποκατάστασης τα οποία είναι απαραίτητα για την επίτευξη συμμόρφωσης με το PCI DSS βαρύνουν εσάς.

Τα έξοδα για την εφαρμογή των βημάτων αποκατάστασης τα οποία είναι απαραίτητα για την επίτευξη συμμόρφωσης με το PCI DSS βαρύνουν εσάς.

Η American Express δεν θα σας επιβάλλει τέλη μη επικύρωσης (που περιγράφονται παρακάτω) για μη συμμόρφωση πριν από την ημερομηνία αποκατάστασης, αλλά εξακολουθείτε να είστε υπεύθυνοι έναντι της American Express για όλες τις υποχρεώσεις αποζημίωσης για Περιστατικό Παραβίασης Δεδομένων και υπόκεισθε σε όλες τις άλλες διατάξεις αυτής της πολιτικής.

Προς αποφυγή κάθε αμφιβολίας, οι Έμποροι που δεν συμμορφώνονται με το PCI DSS δεν είναι επιλέξιμοι για το πρόγραμμα STEP.

#### Βήμα 4: Στείλτε την Τεκμηρίωση Επικύρωσης στην American Express

Όλοι οι Έμποροι και οι Πάροχοι Υπηρεσιών που απαιτείται να εγγραφούν στο Πρόγραμμα πρέπει να υποβάλλουν την Τεκμηρίωση Επικύρωσης η οποία έχει επισημανθεί ως «υποχρεωτική» στους πίνακες στο [Βήμα 2: «Προσδιορίστε το Επίπεδο Εμπόρου στο οποίο υπάγεστε και τις Απαιτήσεις Επικύρωσης»](#) στην American Express μέχρι την ισχύουσα προθεσμία.

Πρέπει να υποβάλλετε την Τεκμηρίωση Επικύρωσης στην American Express χρησιμοποιώντας την Πύλη που παρέχεται από τον Διαχειριστή του Προγράμματος ο οποίος επιλέγεται από την American Express. Υποβάλλοντας την Τεκμηρίωση Επικύρωσης, δηλώνετε και διαβεβαιώνετε την American Express ότι τα παρακάτω είναι αληθή (όσο καλύτερα μπορείτε):

- Η αξιολόγησή σας ήταν πλήρης και διεξοδική.
- Η κατάσταση PCI DSS αποτυπώνεται με ακρίβεια τη στιγμή της ολοκλήρωσης, είτε παρουσιάζει προφίλ συμμόρφωσης είτε όχι.
- Έχετε την εξουσιοδότηση να κοινοποιήσετε τις πληροφορίες που περιέχονται στην παρούσα και παρέχετε την Τεκμηρίωση Επικύρωσης στην American Express χωρίς να παραβιάζετε τα δικαιώματα οποιουδήποτε άλλου μέρους.

#### Τέλη Μη Επικύρωσης και Τερματισμός της Συμφωνίας

Η American Express έχει το δικαίωμα να επιβάλλει σε εσάς τέλη μη επικύρωσης και να τερματίσει τη Συμφωνία εάν δεν εκπληρώνετε αυτές τις προϋποθέσεις ή δεν παρέχετε την υποχρεωτική Τεκμηρίωση Επικύρωσης στην American Express μέχρι την ισχύουσα προθεσμία. Η American Express θα σας ειδοποιήσει ξεχωριστά για την ισχύουσα προθεσμία για κάθε ετήσια και τριμηνιαία περίοδο αναφοράς.

#### Πίνακας Α-6: Τέλος Μη Συμμόρφωσης

Περιγραφή*	Έμπορος Επιπέδου 1 ή Πάροχος Υπηρεσιών Επιπέδου 1	Έμπορος Επιπέδου 2 ή Πάροχος Υπηρεσιών Επιπέδου 2	Έμπορος Επιπέδου 3 ή Επιπέδου 4
Ένα τέλος μη επικύρωσης θα υπολογιστεί εάν η Τεκμηρίωση Επικύρωσης δεν ληφθεί εντός της πρώτης προθεσμίας.	25.000 \$ (USD)	5.000 \$ (USD)	50 \$ (USD)
Ένα πρόσθετο τέλος μη επικύρωσης θα υπολογιστεί εάν η Τεκμηρίωση Επικύρωσης δεν ληφθεί έως τη δεύτερη προθεσμία.	35.000 \$ (USD)	10.000 \$ (USD)	100 \$ (USD)
Ένα πρόσθετο τέλος μη επικύρωσης θα υπολογιστεί εάν η Τεκμηρίωση Επικύρωσης δεν ληφθεί έως την τρίτη προθεσμία. <b>ΣΗΜΕΙΩΣΗ:</b> Τα τέλη μη επικύρωσης θα συνεχίσουν να επιβάλλονται έως την υποβολή της Τεκμηρίωσης Επικύρωσης.	45.000 \$ (USD)	15.000 \$ (USD)	250 \$ (USD)

\* Τα Τέλη Μη Επικύρωσης θα υπολογίζονται σε ισοδύναμα ποσά στο Τοπικό Νόμισμα.

\* Δεν ισχύει για την Αργεντινή.

Εάν δεν ανταποκριθείτε στις υποχρεώσεις σας σε ό,τι αφορά την Τεκμηρίωση Επικύρωσης PCI DSS, τότε η American Express έχει το δικαίωμα να επιβάλει σωρευτικά τέλη μη επικύρωσης, να αναβάλει πληρωμές ή/και να τερματίσει τη Συμφωνία.

## Ενότητα 6

### Εχεμύθεια

Η American Express θα λάβει εύλογα μέτρα για να διατηρήσει (και να αναγκάσει τους αντιπροσώπους της και τους υπεργολάβους της, συμπεριλαμβανομένου του παρόχου υπηρεσιών της Πύλης, να διατηρήσουν) τις εκθέσεις συμμόρφωσής σας, συμπεριλαμβανομένης της Τεκμηρίωσης Επικύρωσης, και να μην αποκαλύψει την Τεκμηρίωση επικύρωσης σε τρίτους (εκτός από θυγατρικές, αντιπροσώπους, Παρόχους Υπηρεσιών και υπεργολάβους της American Express) για μια περίοδο τριών ετών από την ημερομηνία παραλαβής, με εξαίρεση ότι αυτή η υποχρέωση εχεμύθειας δεν ισχύει για τα έγγραφα επικύρωσης που:

- α. είναι ήδη γνωστά στην American Express πριν από την αποκάλυψη·
- β. είναι ήδη ή καθίστανται διαθέσιμα στο κοινό, χωρίς παραβίαση της παρούσας παραγράφου από την American Express·
- γ. παραλαμβάνονται δικαιωματικά από τρίτο μέρος προς την American Express χωρίς υποχρέωση εχεμύθειας·
- δ. αναπτύσσεται ανεξάρτητα από την American Express· ή
- ε. απαιτείται η αποκάλυψή τους με εντολή δικαστηρίου, διοικητικής υπηρεσίας ή κυβερνητικής αρχής ή με οποιονδήποτε νόμο, κανόνα ή κανονισμό ή με κλήση, αίτημα ανακάλυψης, κλήτευση ή άλλη διοικητική ή νομική διαδικασία ή με οποιαδήποτε επίσημη ή ανεπίσημη διερεύνηση ή έρευνα από οποιαδήποτε κυβερνητική υπηρεσία ή αρχή (συμπεριλαμβανομένης οποιασδήποτε ρυθμιστικής αρχής, επιθεωρητή, εξεταστή ή υπηρεσίας επιβολής του νόμου).

## Ενότητα 7

### Δήλωση αποποίησης ευθύνης

Η AMERICAN EXPRESS ΑΠΟΠΟΙΕΙΤΑΙ ΜΕ ΤΟ ΠΑΡΟΝ ΟΠΟΙΟΣΔΗΠΟΤΕ ΕΚΠΡΟΣΩΠΗΣΕΙΣ, ΕΓΓΥΗΣΕΙΣ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ ΟΣΩΝ ΑΦΟΡΑ ΤΗΝ ΠΟΛΙΤΙΚΗ ΛΕΙΤΟΥΡΓΙΑΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ, ΤΟ PCI DSS, ΤΙΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΜΝ ΚΑΙ ΤΗΝ ΟΝΟΜΑΣΙΑ ΚΑΙ ΤΗΝ ΑΠΟΔΟΣΗ ΤΩΝ QSA, ASV Η ΡFI (Η ΟΠΟΙΟΔΗΠΟΤΕ ΑΠΟ ΑΥΤΑ), ΕΙΤΕ ΕΚΦΡΑΣΜΕΝΗΣ, ΕΙΤΕ ΕΝΝΟΟΥΜΕΝΗΣ, ΘΕΣΜΙΚΗΣ Ή ΑΛΛΗΣ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΗΣ ΟΠΟΙΟΣΔΗΠΟΤΕ ΕΓΓΥΗΣΗΣ ΕΜΠΟΡΕΥΣΙΜΟΤΗΤΑΣ Ή ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ ΓΙΑ ΣΥΓΚΕΚΡΙΜΕΝΟ ΣΚΟΠΟ. ΟΙ ΕΚΔΟΤΕΣ ΚΑΡΤΩΝ ΤΗΣ AMERICAN EXPRESS ΔΕΝ ΕΙΝΑΙ ΤΡΙΤΟΙ ΔΙΚΑΙΟΥΧΟΙ ΒΑΣΕΙ ΤΗΣ ΠΑΡΟΥΣΑΣ ΠΟΛΙΤΙΚΗΣ.

## Χρήσιμοι ιστότοποι

Ασφάλεια δεδομένων, American Express: [www.americanexpress.com/datasecurity](http://www.americanexpress.com/datasecurity)

PCI Security Standards Council, LLC: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

## Γλωσσάριο

Για τους σκοπούς της παρούσας [Πολιτικής Λειτουργίας Ασφάλειας Δεδομένων \(DSOP\)](#) μόνο, ισχύουν οι παρακάτω ορισμοί οι οποίοι υπερισχύουν σε περίπτωση διένεξης με τους όρους που αναγράφονται στο έγγραφο *Κανονισμοί για Εμπόρους*.

**Αριθμός Κάρτας** είναι ο μοναδικός αριθμός αναγνώρισης που εκχωρεί ο Εκδότης στην Κάρτα κατά την έκδοσή της.

**Αριθμός Κάρτας που έχει εκτεθεί σε κίνδυνο** είναι ο αριθμός λογαριασμού της κάρτας American Express που σχετίζεται με ένα Περιστατικό Παραβίασης Δεδομένων.

**Βεβαίωση Συμμόρφωσης (AOC)** σημαίνει δήλωση της κατάστασης της συμμόρφωσής σας με το πρότυπο PCI DSS, με τη μορφή που παρέχεται από το Payment Card Industry Security Standards Council, LLC.

**Βεβαίωση Συμμόρφωσης Σάρωσης (AOSC)** σημαίνει δήλωση της κατάστασης της συμμόρφωσής σας με το PCI DSS, βασιζόμενο σε σάρωση δικτύου, με τη μορφή που παρέχεται από το Payment Card Industry Security Standards Council, LLC.

**Δικαιοπάροχος** σημαίνει τον διευθυντή μιας επιχείρησης, η οποία χορηγεί άδεια σε άτομα ή Φορείς (Δικαιοδόχους) με σκοπό να διανέμουν αγαθά ή/και υπηρεσίες με το όνομα του Σήματος του Διευθυντή ή να λειτουργούν με αυτό το όνομα· παρέχει βοήθεια προς τους Δικαιοδόχους για τη διαχείριση της επιχείρησής τους ή επηρεάζει τη μέθοδο λειτουργίας του Δικαιοδόχου· και απαιτεί πληρωμή ενός τέλους από τους Δικαιοδόχους.

**Δικαιούχος** σημαίνει ένα τρίτο μέρος το οποίο τελεί υπό ανεξάρτητη κατοχή και λειτουργία (συμπεριλαμβανομένου ενός δικαιούχου, αδειοδοτημένου μέρους ή τμήματος) εκτός από Θυγατρική η οποία έχει λάβει άδεια από Δικαιοπάροχο για

λειτουργία δικαιόχρησης και έχει συνάψει γραπτή συμφωνία η οποία προβλέπει με συνέπεια την εμφανή εξωτερική ταυτοποίηση με τα Σήματα του Δικαιοπαρόχου ή την παρουσίαση στο ευρύ κοινό ως μέλους ομίλου εταιρειών του Δικαιοπαρόχου.

**Δισημειακή Κρυπτογράφηση (P2PE)** σημαίνει μια λύση που προστατεύει κρυπτογραφικά τα δεδομένα λογαριασμού από το σημείο όπου ο έμπορος αποδέχεται την κάρτα πληρωμής ως το ασφαλές σημείο αποκρυπτογράφησης.

**Εγκεκριμένος Εκτιμητής Ασφαλείας (QSA)** σημαίνει έναν φορέα που έχει πιστοποιηθεί από το Payment Card Industry Security Standards Council, LLC για να επικυρώνει την τήρηση των PCI DSS.

**Εγκεκριμένος Προμηθευτής Σάρωσης (ASV)** σημαίνει ένας φορέας που έχει πιστοποιηθεί από το Payment Card Industry Security Standards Council, LLC (Συμβούλιο Προτύπων Ασφάλειας της Βιομηχανίας Καρτών Πληρωμών) για να επικυρώσει την τήρηση ορισμένων απαιτήσεων PCI DSS, πραγματοποιώντας σαρώσεις τρωτών σημείων σε περιβάλλοντα με διαδίκτυο.

**Εγκληματολογικός Ερευνητής PCI (PFI)** σημαίνει έναν φορέα που έχει εγκριθεί από το Payment Card Industry Security Standards Council, LLC (Συμβούλιο Προτύπων Ασφάλειας της Βιομηχανίας Καρτών Πληρωμών) για την πραγματοποίηση εγκληματολογικών ερευνών για παραβίαση ή διακινδύνευση δεδομένων καρτών πληρωμών.

**Εκδότης** σημαίνει έναν Φορέα (συμπεριλαμβανομένης της American Express και των θυγατρικών της) ο οποίος έχει λάβει άδεια από την American Express ή μια θυγατρική της American Express για την έκδοση Καρτών και τη συμμετοχή σε επιχειρηματικές δραστηριότητες έκδοσης Καρτών.

**Έμπορος** σημαίνει τον έμπορο και όλες τις θυγατρικές του που δέχονται κάρτες American Express βάσει συμφωνίας με την American Express ή τις θυγατρικές της.

**Έμπορος Επιπέδου 1** σημαίνει έναν Έμπορο με 2,5 εκατομμύρια Συναλλαγές Κάρτας American Express ή περισσότερες ανά έτος· ή οποιοσδήποτε Έμπορος που η American Express κρίνει ότι εντάσσεται στο Επίπεδο 1.

**Έμπορος Επιπέδου 2** σημαίνει έναν Έμπορο με 50.000 έως 2,5 εκατομμύρια Συναλλαγές Κάρτας American Express ανά έτος.

**Έμπορος Επιπέδου 3** σημαίνει έναν Έμπορο με 10.000 έως 50.000 Συναλλαγές Κάρτας American Express ανά έτος.

**Έμπορος Επιπέδου 4** σημαίνει έναν Έμπορο με κάτω από 10.000 συναλλαγές κάρτας American Express ανά έτος.

**Επεξεργαστής** σημαίνει έναν πάροχο υπηρεσιών προς τους Εμπόρους, ο οποίος διευκολύνει την έγκριση και την υποβολή της επεξεργασίας στο δίκτυο της American Express.

**Επίπεδο Εμπόρου** είναι η κατηγορία στην οποία κατατάσσουμε τους Εμπόρους και η οποία σχετίζεται με τις υποχρεώσεις επικύρωσης της συμμόρφωσης με το PCI DSS, όπως περιγράφεται στην [Ενότητα 5, «Σημαντική περιοδική επικύρωση των συστημάτων σας»](#).

**Η Αίτηση Πληρωμής** έχει την έννοια που της δόθηκε στο τότε ισχύον Γλωσσάριο Όρων για το Πρότυπο Ασφαλούς Λογισμικού και το Πρότυπο Διάρκειας Ζωής Ασφαλούς Λογισμικού Καρτών Πληρωμής, το οποίο διατίθεται στη διεύθυνση [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Η Εγκεκριμένη Λύση Δισημειακής Κρυπτογράφησης (P2PE)**, περιλαμβάνεται στον κατάλογο επικυρωμένων λύσεων PCI SSC ή έχει επικυρωθεί από μια εταιρεία PCI SSC με Εγκεκριμένο Εκτιμητή Ασφάλειας P2PE.

**Ημερομηνία Ειδοποίησης** σημαίνει την ημερομηνία κατά την οποία η American Express παρέχει στους εκδότες την τελική κοινοποίηση ενός Περιστατικού Παραβίασης Δεδομένων. Η ημερομηνία αυτή εξαρτάται από την παραλαβή της τελικής εγκληματολογικής αναφοράς ή εσωτερικής ανάλυσης από την American Express και καθορίζεται κατά την αποκλειστική κρίση της American Express.

**Η Συσκευή Εισαγωγής PIN** έχει την έννοια που της δόθηκε στο τότε ισχύον Γλωσσάριο Όρων για το Σημείο αλληλεπίδρασης (Point of Interaction, POI) για Ασφάλεια Συναλλαγών της Βιομηχανίας Καρτών Πληρωμών (PIN Transaction Security, PTS), που υπάρχει στη διεύθυνση [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Κάρτα American Express** ή απλώς **Κάρτα**, σημαίνει κάθε κάρτα, συσκευή πρόσβασης λογαριασμού ή συσκευή πληρωμής ή υπηρεσία που φέρει την ονομασία, το λογότυπο, το εμπορικό σήμα, το σήμα υπηρεσίας, την εμπορική επωνυμία ή άλλο ιδιόκτητο σχέδιο ή ονομασία της American Express ή θυγατρικής και εκδίδεται από έναν εκδότη ή έναν αριθμό λογαριασμού κάρτας.

**Κάρτα με Τσιπ** σημαίνει μια Κάρτα που περιέχει ένα τσιπ και θα μπορούσε να απαιτήσει έναν κωδικό PIN ως μέσο επαλήθευσης της ταυτότητας του κατόχου κάρτας ή των πληροφοριών του λογαριασμού που περιέχονται στο τσιπ ή και

τα δύο (μερικές φορές αποκαλείται «έξυπνη κάρτα», «κάρτα EMV» ή «ICC» ή «κάρτα ολοκληρωμένου κυκλώματος» στο υλικό μας).

**Κάτοχος Κάρτας** σημαίνει ένα άτομο ή φορέας (i) που έχει συνάψει συμφωνία δημιουργίας λογαριασμού Κάρτας με έναν εκδότη ή (ii) του οποίου το όνομα εμφανίζεται στην Κάρτα.

**Κλειδί Κρυπτογράφησης (Κλειδί κρυπτογράφησης της American Express)** σημαίνει όλα τα κλειδιά που χρησιμοποιούνται κατά την επεξεργασία, δημιουργία, φόρτωση ή/και προστασία των δεδομένων λογαριασμού. Αυτό περιλαμβάνει, χωρίς περιορισμό, τα παρακάτω:

- Βασικά κλειδιά κρυπτογράφησης: Κύρια Κλειδιά Ζώνης (Zone Master Key, ZMK) και Κλειδιά Pin Ζώνης (Zone Pin Key, ZPK)
- Κύρια κλειδιά που χρησιμοποιούνται σε ασφαλείς συσκευές κρυπτογράφησης: Τοπικά Κύρια Κλειδιά (Local Master Key, LMK)
- Κλειδιά Κωδικού Ασφαλείας Καρτών (Card Security Code Key, CSCCK)
- Κλειδιά PIN: Βασικά κλειδιά εξαγωγής (Base Derivation Key, BDK), κλειδί κρυπτογράφησης PIN (PIN Encryption Key, PEK) και ZPK

**Με τον όρο Εγκεκριμένη βάσει PCI** νοείται ότι μια Συσκευή Εισαγωγής PIN ή μια Εφαρμογή Πληρωμής (ή και τα δύο) εμφανίζεται κατά τη στιγμή χρήσης στον κατάλογο των εγκεκριμένων εταιρειών και παρόχων που τηρούνται από το Security Standards Council, LLC του PCI, το οποίο διατίθεται στη διεύθυνση [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Ο Πρωτεύων Αριθμός Λογαριασμού (PAN)** έχει την έννοια που του δόθηκε στο τότε τρέχον Γλωσσάριο Όρων για το PCI DSS.

**Οι προϋποθέσεις για το Συμβούλιο Προτύπων Ασφάλειας της Βιομηχανίας Καρτών Πληρωμών (Payment Card Industry Security Standards Council, PCI SSC)** είναι ένα σύνολο προτύπων και προϋποθέσεων που αφορούν τη διασφάλιση και την προστασία των δεδομένων των καρτών πληρωμής, μεταξύ των οποίων τα πρότυπα PCI DSS και PA DSS, που διατίθενται στη διεύθυνση [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Παράθυρο Συμβάντος Περιστατικού Παραβίασης Δεδομένων** νοείται η περίοδος της εισβολής (ή χρονική περίοδος που καθορίζεται με παρόμοιο τρόπο) η οποία ορίζεται στην τελική αναφορά εγκληματολογικής έρευνας (π.χ. αναφορά PFI), ή εάν είναι άγνωστη, μια περίοδος έως 365 ημέρες πριν από την Ημερομηνία της τελευταίας Ειδοποίησης για την έκθεση των Αριθμών Κάρτας που είναι πιθανό να έχουν εκτεθεί σε κίνδυνο λόγω εμπλοκής τους στο περιστατικό Διακινδύνευσης Δεδομένων που αναφέρθηκε σε εμάς.

**Πάροχοι Υπηρεσιών** είναι οι εξουσιοδοτημένοι επεξεργαστές, τρίτοι επεξεργαστές, πάροχοι πύλης, ολοκληρωτές συστημάτων POS και οποιοσδήποτε άλλος πάροχος προς Εμπόρους συστημάτων POS ή άλλων λύσεων ή υπηρεσιών επεξεργασίας πληρωμών.

**Πάροχος Υπηρεσιών Επιπέδου 1** σημαίνει έναν Πάροχο Υπηρεσιών με 2,5 εκατομμύρια Συναλλαγές Κάρτας American Express ή περισσότερες ανά έτος, ή οποιονδήποτε Πάροχο Υπηρεσιών που η American Express κρίνει ότι εντάσσεται στο Επίπεδο 1.

**Πάροχος Υπηρεσιών Επιπέδου 2** σημαίνει έναν Πάροχο Υπηρεσιών με λιγότερο από 2,5 εκατομμύρια Συναλλαγές με Κάρτες American Express ανά έτος·ή οποιοσδήποτε Πάροχος Υπηρεσιών δεν κρίνεται ως Επίπεδο 1 από την American Express.

**Περιβάλλον Δεδομένων Κατόχου Κάρτας (CDE)** είναι τα άτομα, οι διαδικασίες και η τεχνολογία που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα του κατόχου κάρτας ή ευαίσθητα δεδομένα αυθεντικοποίησης.

**Περιστατικό Παραβίασης Δεδομένων** σημαίνει ένα συμβάν που συνεπάγεται διακινδύνευση ή υποψία διακινδύνευσης κλειδιών κρυπτογράφησης της American Express ή τουλάχιστον έναν αριθμό λογαριασμού κάρτας American Express στον οποίο υπάρχει:

- μη εξουσιοδοτημένη πρόσβαση ή χρήση κλειδιών κρυπτογράφησης, Στοιχείων Κατόχου Κάρτας ή Ευαίσθητων Δεδομένων Αυθεντικοποίησης (ή συνδυασμός αυτών) που αποθηκεύονται, υποβάλλονται σε επεξεργασία ή μεταδίδονται στον εξοπλισμό, τα συστήματα ή/και τα δίκτυά σας (ή τα εξαρτήματά τους) ή τη χρήση των οποίων έχετε εξουσιοδοτήσει ή παράσχει ή καταστήσει εφικτή·
- χρήση τέτοιων Κλειδιών Κρυπτογράφησης, Στοιχείων Κατόχου Κάρτας ή Ευαίσθητων Δεδομένων Αυθεντικοποίησης (ή συνδυασμός εκάστου), εκτός από όσα προβλέπονται από τη Συμφωνία· ή/και



- υποψία ή επιβεβαίωση απώλειας, κλοπής ή υπεξαίρεσης με οποιονδήποτε τρόπο οποιουδήποτε μέσου, υλικού, αρχείων ή πληροφοριών που περιέχουν αυτά τα Κλειδιά Κρυπτογράφησης, Στοιχεία Κατόχου Κάρτας ή Ευαίσθητα Δεδομένα Αυθεντικοποίησης (ένας συνδυασμός καθενός εξ αυτών).

**Πίστωση** σημαίνει το ποσό της χρέωσης που επιστρέφεται στους Κατόχους Κάρτας για αγορές ή πληρωμές που πραγματοποιούνται με την Κάρτα.

**Πληροφορίες Κατόχου Κάρτας** σημαίνει πληροφορίες σχετικά με τις κάρτες American Express και τις συναλλαγές με κάρτες, συμπεριλαμβανομένων ονομάτων, διευθύνσεων, αριθμών λογαριασμών καρτών και αριθμών αναγνώρισης καρτών (Card Identification, CID).

**Πρόγραμμα, Το** σημαίνει το Πρόγραμμα Συμμόρφωσης PCI της American Express.

**Πρόγραμμα Ενίσχυσης Τεχνολογίας Ασφάλειας (STEP)** σημαίνει το πρόγραμμα της American Express βάσει του οποίου οι Έμποροι ενθαρρύνονται να χρησιμοποιούν τεχνολογίες που βελτιώνουν την ασφάλεια των δεδομένων.

**Πρόγραμμα Στοχευμένης Ανάλυσης** σημαίνει ένα πρόγραμμα το οποίο παρέχει έγκαιρο εντοπισμό μιας δυνητικής διακινδύνευσης δεδομένων Κατόχου Κάρτας στο Περιβάλλον Δεδομένων Κατόχου Κάρτας (CDE). Βλ. [Ενότητα 1. «Πρόγραμμα Στοχευμένης Ανάλυσης \(TAP\)»](#).

**Προδιαγραφές EMV** σημαίνει τις προδιαγραφές που εκδίδονται από τον φορέα EMVCo, LLC, οι οποίες είναι διαθέσιμες στη διεύθυνση [www.emvco.com](http://www.emvco.com).

**Πρότυπο Ασφάλειας Δεδομένων Καρτών Πληρωμής (Payment Card Industry Data Security Standard, PCI DSS)** σημαίνει το Πρότυπο Ασφάλειας Δεδομένων Καρτών Πληρωμής το οποίο είναι διαθέσιμο στη διεύθυνση [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Προϋποθέσεις Ασφάλειας PIN του PCI** σημαίνει τις Προϋποθέσεις Ασφάλειας PIN της βιομηχανίας καρτών πληρωμών, που υπάρχουν στη διεύθυνση [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Πύλη, Η** σημαίνει το σύστημα αναφοράς που παρέχεται από τον διαχειριστή του Προγράμματος PCI της American Express ο οποίος επιλέγεται από την American Express. Οι Έμποροι και οι Πάροχοι Υπηρεσιών είναι υποχρεωμένοι να χρησιμοποιούν Την Πύλη για την υποβολή τεκμηρίωσης επικύρωσης PCI στην American Express.

**PCI DSS** σημαίνει το Πρότυπο Ασφάλειας Δεδομένων Καρτών Πληρωμής, το οποίο είναι διαθέσιμο στη διεύθυνση [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Συναλλαγές Πληρωμών με Πρωτοβουλία Επιχειρήσεων (BIP)** σημαίνει μια συναλλαγή πληρωμής που είναι εφικτή μέσω ενός αρχείου εντολής πληρωμής το οποίο υποβάλλεται σε επεξεργασία μέσω BIP.

**Συσκευή με Δυνατότητα για Τσιπ** σημαίνει μια Συσκευή σε σημείο πώλησης με Δυνατότητα για Τσιπ που έχει έγκυρη και τρέχουσα έγκριση/πιστοποίηση από την EMVCo ([www.emvco.com](http://www.emvco.com)) και είναι ικανή για επεξεργασία συναλλαγών με τσιπ που συμμορφώνονται με το AEIPS.

**Συμβαλλόμενα Μέρη που Καλύπτονται** είναι οποιοσδήποτε ή όλοι οι υπάλληλοι, οι αντιπρόσωποι, οι υπεργολάβοι, οι Επεξεργαστές, οι Πάροχοι Υπηρεσιών, οι προμηθευτές του εξοπλισμού που διαθέτετε στο σημείο πώλησης (POS) ή των συστημάτων ή οι λύσεις επεξεργασίας πληρωμών, οι οντότητες που σχετίζονται με τον εμπορικό σας λογαριασμό στην American Express και οποιοδήποτε άλλο μέρος, προς τους οποίους μπορείτε να παρέχετε πρόσβαση στις Πληροφορίες του κατόχου κάρτας σύμφωνα με τη Συμφωνία.

**Συναλλαγή EMV** σημαίνει μια συναλλαγή με κάρτα με ενσωματωμένο κύκλωμα (που μερικές φορές αποκαλείται «IC Card», «κάρτα με τσιπ», «έξυπνη κάρτα», «κάρτα EMV», ή «ICC») που διεξάγεται σε ένα σημείο πώλησης με τερματικό που δέχεται κάρτα IC (POS) με έγκυρη και εν ισχύ έγκριση τύπου EMV. Οι εγκρίσεις τύπου EMV είναι διαθέσιμες στη διεύθυνση [www.emvco.com](http://www.emvco.com).

**Σύστημα Σημείου Πώλησης (POS)** σημαίνει ένα σύστημα ή έναν εξοπλισμό επεξεργασίας πληροφοριών, συμπεριλαμβανομένου ενός τερματικού, ενός προσωπικού υπολογιστή, ηλεκτρονικής ταμειακής μηχανής, αναγνώστη ανέπαφων συναλλαγών ή μηχανή ή διαδικασία πληρωμής, που χρησιμοποιείται από έναν Έμπορο, για λήψη εξουσιοδοτήσεων ή για συλλογή δεδομένων συναλλαγής ή και των δύο.

**Συναλλαγή** σημαίνει χρέωση ή πίστωση που συμπληρώνεται μέσω μιας Κάρτας.

**Τα Στοιχεία Κατόχου Κάρτας** έχουν την έννοια που τους δόθηκε στο τότε τρέχον Γλωσσάριο Όρων για το PCI DSS.

**Τσιπ** σημαίνει ένα ολοκληρωμένο μικροτσιπ ενσωματωμένο σε μια Κάρτα που περιέχει πληροφορίες Κατόχου Κάρτας και πληροφορίες λογαριασμού.

**Τεχνολογία Μετρίασης Κινδύνων** σημαίνει λύσεις τεχνολογίας που βελτιώνουν την ασφάλεια των Στοιχείων Κατόχων Κάρτας American Express και Ευαίσθητων Δεδομένων Αυθεντικοποίησης, όπως καθορίζεται από την American Express. Για να θεωρηθείτε ότι διαθέτετε Τεχνολογία Μετρίασης Κινδύνων, πρέπει να αποδείξετε την αποτελεσματική χρήση της τεχνολογίας σύμφωνα με τον σχεδιασμό και τον προορισμό της. Ενδεικτικά παραδείγματα, μεταξύ άλλων: EMV, δισημειακή κρυπτογράφηση και δημιουργία εικονικών νομισμάτων (tokenisation).

**Το Ερωτηματολόγιο Αυτοαξιολόγησης (SAQ)** είναι ένα εργαλείο αυτοαξιολόγησης που δημιουργήθηκε από το Payment Card Industry Security Standards Council, LLC, το οποίο αποσκοπεί στην αξιολόγηση και πιστοποίηση συμμόρφωσης με το PCI DSS.

**Τα Ευαίσθητα Δεδομένα Αυθεντικοποίησης** έχουν την έννοια που τους δόθηκε στο τότε τρέχον Γλωσσάριο Όρων για το PCI DSS.

**Τεκμηρίωση Επικύρωσης** είναι το AOC που παρέχεται σε σχέση με την ετήσια επιτόπια αξιολόγηση ασφάλειας ή το SAQ, το AOSC και τις περιλήψεις των ευρημάτων που παρέχονται σε σχέση με τις Τριμηνιαίες Σαρώσεις Δικτύου ή την Ετήσια Πιστοποίηση του Προγράμματος Ενίσχυσης Τεχνολογίας Ασφάλειας.

**Υπόδειγμα Τελικής Αναφοράς Εγκληματολογικού Συμβάντος** σημαίνει το υπόδειγμα που διατίθεται από το PCI Security Standards Council στην ηλ. διεύθυνση [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Χρέωση** σημαίνει μια πληρωμή ή αγορά που γίνεται με μια Κάρτα.

**Ψηφιακό τεκμήριο (token)** σημαίνει το κρυπτογραφικό τεκμήριο (token) το οποίο αντικαθιστά τον PAN βάσει ενός δεδομένου δείκτη για μια μη προβλέψιμη τιμή.