ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ

ΕΥΡΩΣΥΣΤΗΜΑ

Η ΕΚΤΕΛΕΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

ΠΡΑΞΗ ΕΚΤΕΛΕΣΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΑΡΙΘΜ. 59/18.1.2016

Θέμα: Υιοθέτηση των κατευθυντήριων γραμμών της Ευρωπαϊκής Αρχής Τραπεζών (ΕΑΤ) σχετικά με την ασφάλεια των πληρωμών μέσω διαδικτύου (EBA/GL/2014/12)

Η ΕΚΤΕΛΕΣΤΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΣ ΤΡΑΠΕΖΑΣ ΤΗΣ ΕΛΛΑΔΟΣ, αφού έλαβε υπόψη:

α) το άρθρο 55Α του Καταστατικού της Τράπεζας της Ελλάδος,

β) τις διατάξεις του ν. 4261/2014 «Πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων (ενσωμάτωση της Οδηγίας 2013/36/ΕΕ), κατάργηση του ν. 3601/2007 και άλλες διατάξεις» (ΦΕΚ Α' 107), και ιδίως την παρ. 4 του άρθρου 4, την παρ. 1 του άρθρου 66, τις παρ. 1 και 6 του άρθρου 153 αυτού,

γ) τις διατάξεις του ν. 3862/2010 «Προσαρμογή της ελληνικής νομοθεσίας στις Οδηγίες 2007/64/ΕΚ, 2007/44/ΕΚ και 2010/16/ΕΕ που αφορούν υπηρεσίες πληρωμών στην εσωτερική αγορά, προληπτική αξιολόγηση προτάσεων απόκτησης συμμετοχής σε επιχειρήσεις του χρηματοπιστωτικού τομέα και άλλες διατάξεις» (ΦΕΚ Α' 113), όπως ισχύει, και ιδίως την παρ. 4 του άρθρου 21 αυτού,

δ) τις διατάξεις του Κεφαλαίου Α' του Δεύτερου Μέρους του ν. 4021/2011 «Ενισχυμένα μέτρα εποπτείας και εξυγίανσης των πιστωτικών ιδρυμάτων – Ρύθμιση Θεμάτων Χρηματοπιστωτικού Χαρακτήρα – Κύρωση της Σύμβασης Πλαίσιο του Ευρωπαϊκού Ταμείου Χρηματοπιστωτικής Σταθερότητας και των τροποποιήσεών της και άλλες διατάξεις» (ΦΕΚ Α' 218), και ιδίως την παρ. 4 του άρθρου 12 αυτού,

ε) τον Κανονισμό (ΕΕ) αριθ. 1093/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Νοεμβρίου 2010 σχετικά με τη σύσταση Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Τραπεζών), την τροποποίηση της απόφασης αριθ. 716/2009/ΕΚ και την κατάργηση της απόφασης 2009/78/ΕΚ της Επιτροπής, (ΕΕ L 331/12, 15.12.2010), όπως ισχύει, και ιδίως το άρθρο 16 αυτού,

στ) τις από 19.12.2014 κατευθυντήριες γραμμές της Ευρωπαϊκής Τραπεζικής Αρχής (ΕΑΤ) σχετικά με την ασφάλεια των πληρωμών μέσω διαδικτύου (Final Guidelines on the security of internet payments, EBA/GL/2014/12),

ζ) ότι από τις διατάξεις της παρούσας Πράξης δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού,

Α Π Ο Φ Α Σ Ι Ζ Ε Ι

να καθορίσει τις βασικές γενικές αρχές και κριτήρια, όπως εξειδικεύονται στα πιο κάτω κεφάλαια της παρούσας Πράξης, τα οποία θα πρέπει να πληρούνται από τα

ιδρύματα που παρέχουν υπηρεσίες πληρωμών μέσω διαδικτύου, σε ατομική καθώς και σε ενοποιημένη βάση, προκειμένου να διασφαλίζεται ότι διαθέτουν εσωτερικές λεπτομερείς πολιτικές ασφάλειας, επαρκές σύστημα εσωτερικού ελέγχου και εφαρμόζουν επαρκή μέτρα ασφάλειας, έκτακτης ανάγκης, διαχείρισης περιστατικών και αδιάλειπτης λειτουργίας. Η συμμόρφωση προς τις απαιτήσεις της παρούσας, οι οποίες αποτελούν αναπόσπαστο τμήμα του συστήματος εσωτερικού ελέγχου και της εταιρικής διακυβέρνησης των υπόχρεων προσώπων, γίνεται κατά τρόπο κατάλληλο προς τη φύση, το μέγεθος, το εύρος και την πολυπλοκότητα των δραστηριοτήτων, την εσωτερική οργάνωση και τους κινδύνους που ενέχουν το επιχειρηματικό μοντέλο και οι δραστηριότητες του εποπτευομένου, σύμφωνα με την αρχή της αναλογικότητας.

Ι. Πεδίο εφαρμογής και ορισμοί

1. Οι διατάξεις της παρούσας Πράξης εφαρμόζονται, σε ατομική και σε ενοποιημένη βάση, από τους ακόλουθους παρόχους υπηρεσιών πληρωμών (εφεξής ΠΥΠ):

(α) τα πιστωτικά ιδρύματα με έδρα στην Ελλάδα,

(β) τα υποκαταστήματα των πιστωτικών ιδρυμάτων με έδρα σε χώρα εκτός του Ε.Ο.Χ. που έχουν λάβει άδεια λειτουργίας από την Τράπεζα της Ελλάδος και λειτουργούν στην Ελλάδα,

(γ) τα ιδρύματα πληρωμών με έδρα στην Ελλάδα,

(δ) τα ιδρύματα ηλεκτρονικού χρήματος με έδρα στην Ελλάδα, και

(ε) τις εταιρείες παροχής πιστώσεων με έδρα στην Ελλάδα οι οποίες επιτρέπεται να παρέχουν υπηρεσίες πληρωμών.

2. Οι διατάξεις της παρούσας εφαρμόζονται στις ακόλουθες πράξεις πληρωμών που διενεργούνται μέσω διαδικτύου ανεξαρτήτως της συσκευής πρόσβασης που χρησιμοποιείται:

α) εκτέλεση πράξεων πληρωμών με κάρτα στο διαδίκτυο, συμπεριλαμβανομένων των πληρωμών με άυλη κάρτα, καθώς και καταχώριση των στοιχείων για πληρωμή με κάρτα για χρήση σε «λύσεις πορτοφολιού»,

β) εκτέλεση μεταφορών πίστωσης στο διαδίκτυο,

γ) έκδοση και τροποποίηση ηλεκτρονικών εξουσιοδοτήσεων άμεσης χρέωσης,

δ) μεταφορές ηλεκτρονικού χρήματος μεταξύ δύο λογαριασμών ηλεκτρονικού χρήματος μέσω του διαδικτύου.

3. Διευκρινίζεται ότι στο πεδίο εφαρμογής της παρούσας δεν εμπίπτουν οι ακόλουθες υπηρεσίες:

α) άλλες διαδικτυακές υπηρεσίες -πέραν των αναφερόμενων στην ανωτέρω παράγραφο 2- που τυχόν παρέχει ένας ΠΥΠ μέσω του διαδικτυακού του τόπου πληρωμών (π.χ. ηλεκτρονικές χρηματιστηριακές υπηρεσίες, ηλεκτρονικές συμβάσεις),

β) οι πράξεις πληρωμών η εντολή για την εκτέλεση των οποίων δίνεται μέσω ταχυδρομείου, τηλεφώνου, φωνητικού μηνύματος ή με χρήση τεχνολογίας που βασίζεται σε υπηρεσία σύντομων γραπτών μηνυμάτων (SMS),

γ) οι πράξεις πληρωμών μέσω κινητής συσκευής, με εξαίρεση τις πράξεις πληρωμών που διενεργούνται μέσω προγράμματος περιήγησης,

δ) οι μεταφορές πίστωσης στις περιπτώσεις όπου τρίτο πρόσωπο αποκτά πρόσβαση στον λογαριασμό πληρωμών του πελάτη,

ε) οι πράξεις πληρωμών που πραγματοποιούνται από επιχείρηση μέσω δικτύων ειδικού σκοπού,

στ) οι πράξεις πληρωμών με κάρτα με τη χρήση ανώνυμων και μη επαναφορτιζόμενων φυσικών ή άυλων προπληρωμένων καρτών εφόσον ο εκδότης και ο κάτοχος της κάρτας δεν είναι συμβαλλόμενα-μέρη σύμβασης-πλαισίου , και

ζ) η εκκαθάριση και ο διακανονισμός πράξεων πληρωμής.

4. Για τους σκοπούς της παρούσας Πράξης, και συμπληρωματικά προς τους ορισμούς του ν. 3862/2010, ισχύουν οι ακόλουθοι ορισμοί:

α) «ταυτοποίηση»: η διαδικασία που επιτρέπει στον ΠΥΠ να επαληθεύει την ταυτότητα του πελάτη,

β) «ισχυρή ταυτοποίηση πελάτη»: η διαδικασία που βασίζεται στη χρήση δύο ή περισσότερων στοιχείων από τις ακόλουθες κατηγορίες: γνώσης, κυριότητας και σύμφυτου χαρακτηριστικού του χρήστη:

i) Γνώση: στοιχείο το οποίο γνωρίζει αποκλειστικά ο χρήστης υπηρεσίας πληρωμών π.χ. στατικό συνθηματικό, κωδικός, προσωπικός αριθμός αναγνώρισης (PIN),

ii) Κυριότητα: πράγμα το οποίο αποκλειστικά ο χρήστης υπηρεσίας πληρωμών έχει στην κυριότητά του, π.χ. συσκευή παραγωγής πρόσθετου κωδικού ασφάλειας, έξυπνη κάρτα, κινητό τηλέφωνο,

iii) Εγγενές χαρακτηριστικό: μοναδικό σύμφυτο χαρακτηριστικό του χρήστη υπηρεσίας πληρωμών, π.χ. βιομετρικό χαρακτηριστικό, όπως δακτυλικό αποτύπωμα.

Επιπλέον, τα στοιχεία που επιλέγονται πρέπει να είναι ανεξάρτητα μεταξύ τους, με την έννοια ότι η παραβίαση του ενός δεν θέτει σε κίνδυνο το άλλο ή τα λοιπά. Τουλάχιστον ένα από τα στοιχεία που επιλέγονται δεν πρέπει να μπορεί να επαναχρησιμοποιηθεί ή να αναπαραχθεί (εξαιρουμένων των σύμφυτων χαρακτηριστικών του χρήστη) ή να υποκλαπεί μέσω του διαδικτύου χωρίς να το αντιληφθεί ο χρήστης. Η διαδικασία ισχυρής ταυτοποίησης πρέπει να είναι σχεδιασμένη κατά τρόπο που να προστατεύεται η εμπιστευτικότητα των δεδομένων ταυτοποίησης,

γ) «έγκριση»: η διαδικασία με την οποία ελέγχεται εάν ο πελάτης υπηρεσίας πληρωμών ή ο ΠΥΠ έχει το δικαίωμα να προβεί σε συγκεκριμένη ενέργεια (π.χ. μεταφορά κεφαλαίων, πρόσβαση σε ευαίσθητα δεδομένα),

δ) «διαπιστευτήρια»: οι πληροφορίες εμπιστευτικού χαρακτήρα που παρέχει ο πελάτης ή ο ΠΥΠ για σκοπούς ταυτοποίησης. Ως «διαπιστευτήριο» νοείται επίσης η κατοχή φυσικού εργαλείου που περιέχει τις προαναφερόμενες πληροφορίες (π.χ. συσκευή παραγωγής κωδικών μίας χρήσης, έξυπνη κάρτα) ή στοιχείο που ο χρήστης απομνημονεύει ή στοιχείο που τον αντιπροσωπεύει (όπως τα βιομετρικά χαρακτηριστικά),

ε) «σημαντικό περιστατικό ασφάλειας πληρωμών»: περιστατικό το οποίο έχει ή ενδέχεται να έχει σημαντική επίπτωση στην ασφάλεια, την ακεραιότητα ή τη συνέχεια των συστημάτων του ΠΥΠ που συνδέονται με πληρωμές και/ή στην ασφάλεια των ευαίσθητων δεδομένων πληρωμής ή των κεφαλαίων. Για την αξιολόγηση της σημαντικότητας του περιστατικού λαμβάνεται υπόψη ο αριθμός των πελατών που ενδέχεται να θιγούν, το διακυβευόμενο ποσό και η επίπτωση σε άλλους ΠΥΠ ή σε άλλες υποδομές πληρωμών,

στ) «ανάλυση του κινδύνου της συναλλαγής»: η αξιολόγηση του κινδύνου που αφορά συγκεκριμένη συναλλαγή, στο πλαίσιο της οποίας λαμβάνονται υπόψη κριτήρια όπως τα συναλλακτικά πρότυπα (συμπεριφορά) του πελάτη όσον αφορά τις πληρωμές, η αξία της σχετικής συναλλαγής, το είδος του προϊόντος και το προφίλ του δικαιούχου,

ζ) «άυλες κάρτες»: λύση πληρωμής που βασίζεται σε κάρτα, στο πλαίσιο της οποίας δημιουργείται ένας εναλλακτικός, προσωρινός αριθμός κάρτας με περιορισμένη περίοδο ισχύος, περιορισμένη χρήση και προκαθορισμένο όριο δαπανών, που μπορεί να χρησιμοποιηθεί για την πραγματοποίηση αγορών στο διαδίκτυο,

η) «λύσεις πορτοφολιού»: λύσεις που παρέχουν τη δυνατότητα σε έναν πελάτη να καταχωρίζει δεδομένα που αφορούν ένα ή περισσότερα μέσα πληρωμών προκειμένου να προβαίνει σε πληρωμές προς διάφορες επιχειρήσεις ηλεκτρονικού εμπορίου.

II. Γενικό περιβάλλον ελέγχου και ασφάλειας

Α. Διακυβέρνηση

1. Το Διοικητικό Συμβούλιο των ΠΥΠ εγκρίνει, επιβλέπει την εφαρμογή και είναι αρμόδιο για την αναθεώρηση σε τακτική βάση της επίσημης πολιτικής ασφάλειας του ιδρύματος για τις υπηρεσίες πληρωμών μέσω διαδικτύου.

2. Η πολιτική ασφάλειας είναι δεόντως καταγεγραμμένη, υπόκειται σε αναθεώρηση ανά τακτά χρονικά διαστήματα (σύμφωνα με την παράγραφο 5 του ακόλουθου Κεφαλαίου Β της παρούσας Πράξης) και καθορίζει τους στόχους ασφάλειας και τη διάθεση ανάληψης κινδύνων του ιδρύματος.

3. Η πολιτική ασφάλειας προσδιορίζει τους ρόλους, τις αρμοδιότητες, περιλαμβανομένης της λειτουργίας διαχείρισης του κινδύνου η οποία αναφέρεται απευθείας στο Διοικητικό Συμβούλιο, καθώς και τις γραμμές αναφοράς για τις παρεχόμενες υπηρεσίες πληρωμών μέσω του διαδικτύου, περιλαμβανομένης της διαχείρισης ευαίσθητων δεδομένων πληρωμής όσον αφορά την αξιολόγηση, τον έλεγχο και την μείωση των κινδύνων.

Β. Αξιολόγηση του κινδύνου

1. Οι ΠΥΠ διενεργούν και τεκμηριώνουν λεπτομερείς αξιολογήσεις κινδύνου όσον αφορά την ασφάλεια των πληρωμών μέσω του διαδικτύου και των συναφών υπηρεσιών, τόσο πριν από τη δημιουργία της υπηρεσίας (ή των υπηρεσιών) όσο και ανά τακτά χρονικά διαστήματα στη συνέχεια.

2. Η λειτουργία διαχείρισης κινδύνων των ΠΥΠ διενεργεί και τεκμηριώνει λεπτομερείς αξιολογήσεις κινδύνου για τις πληρωμές μέσω διαδικτύου και τις συναφείς υπηρεσίες. Οι ΠΥΠ εξετάζουν τα αποτελέσματα της συνεχούς παρακολούθησης των απειλών κατά της ασφάλειας των υπηρεσιών πληρωμών μέσω διαδικτύου που προσφέρουν ή σχεδιάζουν να προσφέρουν, λαμβάνοντας υπόψη:

α) τις τεχνολογικές λύσεις που χρησιμοποιούν,

β) τις υπηρεσίες που αναθέτουν σε εξωτερικούς παρόχους, και

γ) το τεχνικό περιβάλλον των πελατών.

Οι ΠΥΠ εξετάζουν τους κινδύνους που συνδέονται με τις χρησιμοποιούμενες εκ μέρους τους τεχνολογικές πλατφόρμες, με την αρχιτεκτονική των εφαρμογών, με τις τεχνικές και τις ρουτίνες προγραμματισμού τόσο από τη δική τους πλευρά ως παρόχων (όπως κινδύνους ευαισθησίας του συστήματος σε επιθέσεις υφαρπαγής συνόδου (session hijacking), προσθήκης κακόβουλου κώδικα SQL (SQL injection), επίθεσης μέσω δέσμης ενεργειών από άλλη τοποθεσία (cross-site scripting), υπερχείλισης προσωρινής μνήμης (buffer overflow)) όσο και από την πλευρά των

πελατών τους όπως κινδύνους που συνδέονται με τη χρήση εφαρμογών πολυμέσων, προσθηκών για προγράμματα περιήγησης, πλαισίων, εξωτερικών συνδέσμων κ.λπ., καθώς και τα ευρήματα που προκύπτουν από τη διαδικασία παρακολούθησης περιστατικών ασφάλειας όπως αυτά αναφέρονται στο Κεφάλαιο Γ του παρόντος Τίτλου.

3. Βάσει των ανωτέρω, οι ΠΥΠ καθορίζουν κατά πόσον και σε ποιον βαθμό ενδέχεται να απαιτούνται αλλαγές στα υπάρχοντα μέτρα ασφάλειας, στις τεχνολογίες που χρησιμοποιούνται και στις διαδικασίες ή τις υπηρεσίες που προσφέρονται. Οι ΠΥΠ λαμβάνουν υπόψη τον χρόνο που απαιτείται για την εφαρμογή των αλλαγών (περιλαμβανομένου του χρόνου της υιοθέτησής τους από τους πελάτες) και λαμβάνουν τα κατάλληλα προσωρινά μέτρα για την ελαχιστοποίηση των περιστατικών ασφάλειας και απάτης, καθώς και των ενδεχόμενων δυσλειτουργιών.

4. Η αξιολόγηση των κινδύνων καλύπτει την ανάγκη προστασίας και διασφάλισης των ευαίσθητων δεδομένων των πληρωμών.

5. Οι ΠΥΠ προβαίνουν σε επανεξέταση των σεναρίων κινδύνου και των υφιστάμενων μέτρων ασφάλειας ύστερα από σημαντικά περιστατικά που επηρεάζουν τις υπηρεσίες τους, πριν από την πραγματοποίηση σημαντικών αλλαγών στην υποδομή ή στις διαδικασίες και μετά από τον εντοπισμό νέων απειλών μέσω διαδικασιών παρακολούθησης του κινδύνου. Επιπλέον, διενεργούν τουλάχιστον μία φορά ετησίως γενική επανεξέταση της αξιολόγησης του κινδύνου. Τα αποτελέσματα των αξιολογήσεων κινδύνου και των επανεξετάσεων υποβάλλονται προς έγκριση στο Διοικητικό Συμβούλιο των ΠΥΠ.

Γ. Παρακολούθηση και αναφορά περιστατικών

1. Οι ΠΥΠ διασφαλίζουν τη συνεπή και ολοκληρωμένη παρακολούθηση και διαχείριση των συμβάντων ασφάλειας, συμπεριλαμβανομένων των καταγγελιών των πελατών σχετικά με την ασφάλεια και δημιουργούν διαδικασίες για την αναφορά τέτοιων περιστατικών στη διοίκησή τους και, στην περίπτωση σημαντικών περιστατικών ασφάλειας πληρωμών, στην Τράπεζα της Ελλάδος.

2. Οι ΠΥΠ εφαρμόζουν διαδικασίες για τον έλεγχο, τον χειρισμό και την παρακολούθηση των περιστατικών ασφάλειας και των καταγγελιών πελατών που αφορούν θέματα ασφάλειας και να αναφέρουν τα περιστατικά αυτά στη διοίκηση.

3. Οι ΠΥΠ εφαρμόζουν διαδικασίες για την άμεση ενημέρωση της Τράπεζας της Ελλάδος και της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, σε περίπτωση σημαντικών περιστατικών ασφάλειας πληρωμών που σχετίζονται με τις παρεχόμενες υπηρεσίες πληρωμών.

4. Οι ΠΥΠ εφαρμόζουν διαδικασίες για τη συνεργασία με τις αστυνομικές και δικαστικές αρχές όσον αφορά σημαντικά περιστατικά ασφάλειας πληρωμών, συμπεριλαμβανομένων των παραβιάσεων των δεδομένων.

5. Οι ΠΥΠ που αποδέχονται συναλλαγές με κάρτα πρέπει, βάσει σύμβασης, να απαιτούν από τις επιχειρήσεις ηλεκτρονικού εμπορίου που αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν ευαίσθητα δεδομένα πληρωμών να συνεργάζονται, τόσο με τους ίδιους όσο και με τις αντίστοιχες διωκτικές αρχές, σε περιπτώσεις σημαντικών περιστατικών ασφάλειας πληρωμών, συμπεριλαμβανομένων παραβιάσεων δεδομένων. Εάν ο ΠΥΠ διαπιστώσει ότι επιχείρηση ηλεκτρονικού εμπορίου με την οποία συνεργάζεται δεν τηρεί τις συμβατικές της υποχρεώσεις είτε λαμβάνει μέτρα για να εφαρμοστούν οι συμβατικές αυτές υποχρεώσεις ή καταγγέλλει τη σύμβαση.

Δ. Έλεγχος και μείωση των κινδύνων

1. Οι ΠΥΠ εφαρμόζουν μέτρα ασφάλειας σύμφωνα με την αντίστοιχη πολιτική ασφάλειας που ακολουθούν προκειμένου να μειώνουν τους κινδύνους που εντοπίζονται. Τα μέτρα αυτά ενσωματώνουν πολλαπλά επίπεδα ασφάλειας, στο πλαίσιο των οποίων η αποτυχία μίας «γραμμής άμυνας» αντιμετωπίζεται από την επόμενη «γραμμή άμυνας» («εις βάθος άμυνα»).

2. Κατά τον σχεδιασμό, την ανάπτυξη και τη συντήρηση υπηρεσιών πληρωμών μέσω διαδικτύου, οι ΠΥΠ δίνουν ιδιαίτερη προσοχή στον επαρκή διαχωρισμό των καθηκόντων στα περιβάλλοντα τεχνολογίας της πληροφορίας (π.χ. τα περιβάλλοντα ανάπτυξης, δοκιμής και παραγωγής) και στην ορθή εφαρμογή της αρχής των «ελάχιστων προνομίων» ως βάση για τη χρηστή διαχείριση της ταυτότητας και της πρόσβασης.

3. Οι ΠΥΠ διαθέτουν κατάλληλες λύσεις ασφάλειας για την προστασία των δικτύων, των δικτυακών τόπων, των εξυπηρετητών και των ζεύξεων επικοινωνίας από περιστατικά κατάχρησης ή από επιθέσεις. Οι ΠΥΠ αφαιρούν από τους εξυπηρετητές όλες τις περιττές λειτουργίες προκειμένου να τους προστατεύουν, να τους καθιστούν περισσότερο ανθεκτικούς και να εξαλείφουν ή να μειώνουν τα τρωτά σημεία των εφαρμογών που κινδυνεύουν. Η πρόσβαση μέσω των διαφόρων εφαρμογών στα απαραίτητα δεδομένα και πηγές διατηρείται στο απολύτως αναγκαίο επίπεδο με βάση την «αρχή των ελάχιστων προνομίων». Προκειμένου να περιοριστεί η χρήση «πλαστών» δικτυακών τόπων (που μιμούνται νόμιμους δικτυακούς τόπους ΠΥΠ), οι δικτυακοί τόποι συναλλαγών που προσφέρουν υπηρεσίες πληρωμών μέσω διαδικτύου διαθέτουν, για την ταυτοποίησή τους, πιστοποιητικά εκτεταμένης επικύρωσης που εκδίδονται στο όνομα του ΠΥΠ ή εφαρμόζουν άλλες παρόμοιες μεθόδους ταυτοποίησης.

4. Οι ΠΥΠ εφαρμόζουν κατάλληλες διαδικασίες παρακολούθησης, ιχνηλασίας και περιορισμού της πρόσβασης σε: i) ευαίσθητα δεδομένα πληρωμών, και ii) κρίσιμους λογικούς και φυσικούς πόρους, όπως δίκτυα, συστήματα, βάσεις δεδομένων, υποσυστήματα ασφάλειας κ.λπ. Οι ΠΥΠ δημιουργούν, αποθηκεύουν και αναλύουν κατάλληλα αρχεία καταγραφής και ίχνη ελέγχου.

5. Κατά τον σχεδιασμό, την ανάπτυξη και τη συντήρηση υπηρεσιών πληρωμών μέσω διαδικτύου, προς το σκοπό της προστασίας της ιδιωτικότητας οι ΠΥΠ διασφαλίζουν ότι η ελαχιστοποίηση των δεδομένων, ήτοι η συλλογή των ελάχιστων αναγκαίων προσωπικών στοιχείων για την εκτέλεση μιας συγκεκριμένης λειτουργίας, συνιστά ουσιώδες στοιχείο της βασικής λειτουργικότητας. Η συλλογή, η δρομολόγηση, η επεξεργασία, η αποθήκευση και/ή η αρχειοθέτηση, καθώς και η απεικόνιση ευαίσθητων δεδομένων πληρωμών διατηρούνται σε απολύτως αναγκαία επίπεδα, τηρουμένης της οικείας εθνικής νομοθεσίας για την προστασία των προσωπικών δεδομένων.

6. Τα μέτρα ασφάλειας για τις υπηρεσίες πληρωμών μέσω διαδικτύου υποβάλλονται σε δοκιμές υπό την επίβλεψη της λειτουργίας διαχείρισης του κινδύνου προκειμένου να διασφαλίζεται η ανθεκτικότητα και η αποτελεσματικότητά τους. Όλες οι αλλαγές υπόκεινται σε επίσημη διαδικασία διαχείρισης των αλλαγών που να διασφαλίζει ότι οι αλλαγές προγραμματίζονται, υποβάλλονται σε δοκιμές, τεκμηριώνονται και εγκρίνονται δεόντως. Βάσει των αλλαγών που πραγματοποιούνται και των απειλών για την ασφάλεια που παρατηρούνται, οι δοκιμές επαναλαμβάνονται ανά τακτά χρονικά διαστήματα και περιλαμβάνουν σενάρια συναφών και γνωστών πιθανών επιθέσεων.

7. Τα μέτρα ασφάλειας του ΠΥΠ για τις υπηρεσίες πληρωμών μέσω διαδικτύου ελέγχονται περιοδικά για να διασφαλίζεται η ανθεκτικότητα και η αποτελεσματικότητά τους. Επίσης ελέγχονται η υλοποίηση και η λειτουργία των υπηρεσιών διαδικτυακών πληρωμών. Η συχνότητα και η εστίαση των ελέγχων αυτών καθορίζονται λαμβανομένων υπόψη των σχετικών κινδύνων για την ασφάλεια και να είναι αναλογικές προς αυτούς. Οι έλεγχοι διενεργούνται από αξιόπιστους και ανεξάρτητους εμπειρογνώμονες (εσωτερικούς ή εξωτερικούς), οι οποίοι δεν συμμετέχουν κατά κανένα τρόπο στην ανάπτυξη, την εφαρμογή ή την λειτουργική διαχείριση των παρεχόμενων υπηρεσιών πληρωμών μέσω διαδικτύου.

8. Σε κάθε περίπτωση όπου οι ΠΥΠ προβαίνουν σε εξωτερική ανάθεση εργασιών αναφορικά με την ασφάλεια των υπηρεσιών πληρωμών μέσω διαδικτύου, η σχετική σύμβαση ανάθεσης περιλαμβάνει όρους σύμφωνους με τις αρχές και τα κριτήρια που ορίζονται στην παρούσα Πράξη.

9. Οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα πρέπει βάσει σύμβασης να απαιτούν από τις επιχειρήσεις ηλεκτρονικού εμπορίου να

χειρίζονται (δηλαδή να αποθηκεύουν, να επεξεργάζονται και να διαβιβάζουν) τα ευαίσθητα δεδομένα πληρωμών εφαρμόζοντας μέτρα ασφάλειας στις υποδομές πληροφορικής τους, σύμφωνα με τις ανωτέρω παραγράφους 1 έως 8 του παρόντος Κεφαλαίου, προκειμένου να αποτρέπεται η κλοπή των ευαίσθητων αυτών δεδομένων πληρωμών μέσω των συστημάτων τους. Εάν ένας ΠΥΠ διαπιστώσει ότι μια επιχείρηση ηλεκτρονικού εμπορίου δεν εφαρμόζει τα απαραίτητα μέτρα ασφάλειας, λαμβάνει μέτρα για να επιβάλει τη συμβατική αυτή υποχρέωση ή καταγγέλλει τη σύμβαση.

Ε. Ιχνηλασιμότητα

1. Οι ΠΥΠ εφαρμόζουν διαδικασίες με τις οποίες διασφαλίζεται ότι όλες οι συναλλαγές, καθώς και η ροή επεξεργασίας της ηλεκτρονικής εξουσιοδότησης, ιχνηλατούνται δεόντως.

2. Οι ΠΥΠ διασφαλίζουν ότι η υπηρεσία τους ενσωματώνει μηχανισμούς ασφάλειας για τη λεπτομερή καταγραφή των δεδομένων των συναλλαγών και των ηλεκτρονικών εξουσιοδοτήσεων, συμπεριλαμβανομένων του αύξοντος αριθμού των συναλλαγών, χρονοσφραγίδων για τα δεδομένα των συναλλαγών, αλλαγών παραμετροποίησης, καθώς και της πρόσβασης στα δεδομένα των συναλλαγών και των ηλεκτρονικών εξουσιοδοτήσεων.

3. Οι ΠΥΠ διατηρούν αρχεία καταγραφής με τα οποία καθίσταται δυνατή η ιχνηλασία οποιασδήποτε προσθήκης, αλλαγής ή διαγραφής των δεδομένων των συναλλαγών και των ηλεκτρονικών εξουσιοδοτήσεων.

4. Οι ΠΥΠ αντλούν και αναλύουν τα δεδομένα των συναλλαγών και των ηλεκτρονικών εξουσιοδοτήσεων και διασφαλίζουν ότι έχουν στη διάθεσή τους εργαλεία για την αξιολόγηση των αρχείων καταγραφής. Οι αντίστοιχες εφαρμογές είναι διαθέσιμες μόνο σε εξουσιοδοτημένο προσωπικό.

ΙΙΙ. Ειδικά μέτρα ελέγχου και ασφάλειας για τις πληρωμές μέσω διαδικτύου

Α. Αρχική εξακρίβωση ταυτότητας πελάτη, ενημέρωση

1. Η ταυτότητα των πελατών εξακριβώνεται δεόντως σύμφωνα με την κείμενη ελληνική νομοθεσία για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και επιβεβαιώνεται η βούληση των πελατών να προβούν σε πληρωμές μέσω διαδικτύου με χρήση των υπηρεσιών πριν από την παροχή πρόσβασης στις υπηρεσίες αυτές. Οι ΠΥΠ παρέχουν επαρκή προηγούμενη, τακτική ή, κατά περίπτωση ειδική ενημέρωση στον πελάτη σχετικά με τις αναγκαίες προϋποθέσεις (π.χ. εξοπλισμός, διαδικασίες) για την εκτέλεση ασφαλών πράξεων πληρωμής μέσω του διαδικτύου καθώς και σχετικά με τους εγγενείς κινδύνους.

2. Οι ΠΥΠ διασφαλίζουν ότι έχουν εφαρμοστεί όλες οι διαδικασίες δέουσας επιμέλειας ως προς τον πελάτη και ότι ο πελάτης έχει παράσχει επαρκή και γνήσια έγγραφα ταυτότητας (π.χ. διαβατήριο, εθνικό δελτίο ταυτότητας, προηγμένη ηλεκτρονική υπογραφή) και σχετικές πληροφορίες προτού χορηγηθεί σε αυτόν πρόσβαση στις υπηρεσίες πληρωμών μέσω διαδικτύου. Για τη διαδικασία πιστοποίησης και επαλήθευσης της ταυτότητας του πελάτη εφαρμόζονται οι ισχύουσες διατάξεις για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και την καταπολέμηση της τρομοκρατίας περιλαμβανομένων των σχετικών κανονιστικών πράξεων της Τράπεζας της Ελλάδος.

3. Οι ΠΥΠ διασφαλίζουν ότι η προηγούμενη ενημέρωση που παρέχεται στον πελάτη πριν από τη σύναψη σύμβασης για την παροχή υπηρεσιών πληρωμών, πέραν των καθοριζόμενων στο άρθρο 39 του ν. 3862/2010 πληροφοριών, περιλαμβάνει λεπτομερείς πληροφορίες που αφορούν ειδικά τις υπηρεσίες πληρωμών μέσω διαδικτύου. Στις πληροφορίες αυτές περιλαμβάνονται, κατά περίπτωση:

α) σαφείς πληροφορίες σχετικά με τυχόν απαιτήσεις όσον αφορά τον εξοπλισμό, το λογισμικό ή άλλα απαραίτητα εργαλεία που πρέπει να διαθέτει ο πελάτης (π.χ. λογισμικό προστασίας από ιούς, τείχη προστασίας),

β) οδηγίες για την ορθή και ασφαλή χρήση εξατομικευμένων διαπιστευτηρίων ασφάλειας,

γ) αναλυτική περιγραφή κάθε σταδίου της διαδικασίας για την υποβολή και την έγκριση πράξης πληρωμής από τον πελάτη και/ή τη λήψη πληροφοριών, συμπεριλαμβανομένων των συνεπειών κάθε ενέργειας,

δ) οδηγίες για την ορθή και ασφαλή χρήση κάθε υλισμικού και λογισμικού που παρέχεται στον πελάτη,

ε) οι διαδικασίες που ακολουθούνται σε περίπτωση απώλειας ή κλοπής των εξατομικευμένων διαπιστευτηρίων ασφάλειας ή του υλισμικού ή του λογισμικού του πελάτη για την είσοδο στον δικτυακό τόπο ή για την εκτέλεση πράξεων πληρωμής,

στ) οι διαδικασίες που ακολουθούνται εάν εντοπιστεί ή εγερθεί υπόνοια για κατάχρηση,

ζ) περιγραφή των αρμοδιοτήτων και των ευθυνών του ΠΥΠ και του πελάτη αντιστοίχως όσον αφορά τη χρήση της υπηρεσίας πληρωμών μέσω διαδικτύου.

4. Οι ΠΥΠ διασφαλίζουν ότι στη σύμβαση-πλαίσιο που συνάπτουν με τον πελάτη συμφωνείται ότι ο ΠΥΠ μπορεί να αρνείται προσωρινά την εκτέλεση συγκεκριμένης πράξης ή να αναστέλλει τη χρήση του μέσου πληρωμής σύμφωνα με τα οριζόμενα στο άρθρο 52 του ν. 3862/2010 σχετικά με τους περιορισμούς της χρήσης του μέσου πληρωμών για λόγους ασφάλειας. Στη σύμβαση προσδιορίζονται η μέθοδος και οι

όροι ειδοποίησης του πελάτη καθώς και ο τρόπος με τον οποίο ο πελάτης μπορεί να επικοινωνεί με τον ΠΥΠ προκειμένου ο τελευταίος να άρει την προσωρινή άρνηση εκτέλεσης της πράξης ή της υπηρεσίας πληρωμής μέσω διαδικτύου, σύμφωνα με το ν. 3862/2010.

Β. Ισχυρή ταυτοποίηση του πελάτη

1. Η έναρξη πληρωμών μέσω διαδικτύου καθώς και η πρόσβαση σε ευαίσθητα δεδομένα πληρωμών προστατεύεται μέσω της ισχυρής ταυτοποίησης των πελατών. Οι ΠΥΠ εφαρμόζουν διαδικασία ισχυρής ταυτοποίησης των πελατών σύμφωνα με τον ορισμό που παρέχεται στην παρούσα Πράξη.

2. Για τη διενέργεια των υπηρεσιών μεταφοράς πίστωσης, ηλεκτρονικής εξουσιοδότησης και ηλεκτρονικού χρήματος, οι ΠΥΠ προβαίνουν σε ισχυρή ταυτοποίηση του πελάτη για την έγκριση των πράξεων πληρωμής μέσω διαδικτύου του πελάτη (συμπεριλαμβανομένων ομαδοποιημένων μεταφορών πίστωσης) και για την έκδοση ή την τροποποίηση ηλεκτρονικών εξουσιοδοτήσεων άμεσης χρέωσης. Ωστόσο, οι ΠΥΠ θα μπορούσαν να εξετάσουν το ενδεχόμενο θέσπισης εναλλακτικών μέτρων ταυτοποίησης των πελατών για:

α) εξερχόμενες πληρωμές σε έμπιστους δικαιούχους που περιλαμβάνονται σε προϋπάρχουσες λευκές λίστες για τον συγκεκριμένο πελάτη,

β) πράξεις μεταξύ δύο λογαριασμών πληρωμών του ίδιου πελάτη που τηρούνται στον ίδιο ΠΥΠ,

γ) μεταφορές εντός του ίδιου ΠΥΠ που δικαιολογούνται βάσει ανάλυσης του κινδύνου της συναλλαγής,

δ) πληρωμές μικρής αξίας, όπως προσδιορίζονται στην παράγραφο 1 του άρθρου 31 και στην παράγραφο 1 του άρθρου 50 του ν. 3862/2010.

3. Για την απόκτηση πρόσβασης σε ευαίσθητα δεδομένα πληρωμών ή την τροποποίησή τους, συμπεριλαμβανομένης της δημιουργίας και της τροποποίησης λευκών λιστών, απαιτείται ισχυρή ταυτοποίηση του πελάτη. Στις περιπτώσεις όπου ένας ΠΥΠ προσφέρει αμιγώς συμβουλευτικές υπηρεσίες, χωρίς να εμφανίζονται ευαίσθητες πληροφορίες σχετικά με τον πελάτη ή τις πληρωμές, όπως δεδομένα καρτών πληρωμών, που θα μπορούσαν εύκολα να χρησιμοποιηθούν για να διαπραχθεί απάτη, ο ΠΥΠ μπορεί να προσαρμόζει τις απαιτήσεις ταυτοποίησης με βάση την αξιολόγηση του κινδύνου που διενεργεί.

4. Για τις πράξεις πληρωμών με κάρτα, όλοι οι ΠΥΠ που εκδίδουν κάρτες υποστηρίζουν συστήματα ισχυρής ταυτοποίησης του κατόχου της κάρτας. Όλες οι κάρτες που εκδίδονται είναι τεχνικά έτοιμες (καταχωρισμένες) για χρήση με διαδικασία ισχυρής ταυτοποίησης.

5. Οι ΠΥΠ οι οποίοι παρέχουν υπηρεσίες αποδοχής συναλλαγών με κάρτα υποστηρίζουν τεχνολογίες που επιτρέπουν στον εκδότη να εφαρμόζει διαδικασία ισχυρής ταυτοποίησης του κατόχου της κάρτας για τα σχήματα καρτών στα οποία συμμετέχει ο αποδέκτης.

6. Οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα απαιτούν από τις επιχειρήσεις ηλεκτρονικού εμπορίου να υποστηρίζουν λύσεις που επιτρέπουν στον εκδότη να διενεργεί ισχυρή ταυτοποίηση του κατόχου της κάρτας για συναλλαγές με κάρτα μέσω του διαδικτύου. Το ενδεχόμενο χρήσης εναλλακτικών μέτρων ταυτοποίησης θα μπορούσε να εξεταστεί για προκαθορισμένες κατηγορίες συναλλαγών χαμηλού κινδύνου, π.χ. βάσει ανάλυσης του κινδύνου της συναλλαγής ή για πράξεις που αφορούν πληρωμές μικρής αξίας, όπως αυτές προσδιορίζονται στην παράγραφο 1 του άρθρου 31 και στην παράγραφο 1 του άρθρου 50 του ν. 3862/2010.

7. Για τα σχήματα καρτών πληρωμών που δέχεται η υπηρεσία, οι πάροχοι «λύσεων πορτοφολιού» απαιτούν ισχυρή ταυτοποίηση του πελάτη από τον εκδότη όταν ο νόμιμος κάτοχος καταχωρίζει για πρώτη φορά τα στοιχεία της κάρτας.

8. Οι πάροχοι «λύσεων πορτοφολιού» υποστηρίζουν τις διαδικασίες ισχυρής ταυτοποίησης του πελάτη όταν οι πελάτες εισέρχονται στους δικτυακούς τόπους των υπηρεσιών πληρωμών μέσω λύσεων πορτοφολιού ή προβαίνουν σε συναλλαγές με κάρτα μέσω του διαδικτύου. Το ενδεχόμενο χρήσης εναλλακτικών μέτρων ταυτοποίησης θα μπορούσε να εξεταστεί για προκαθορισμένες κατηγορίες συναλλαγών χαμηλού κινδύνου, π.χ. βάσει ανάλυσης του κινδύνου της συναλλαγής, ή για πράξεις που αφορούν πληρωμές μικρής αξίας, όπως αυτές προσδιορίζονται στην παράγραφο 1 του άρθρου 31 και στην παράγραφο 1 του άρθρου 50 του ν. 3862/2010.

9. Για τις άυλες κάρτες, η αρχική καταχώριση πραγματοποιείται σε ασφαλές και αξιόπιστο περιβάλλον. Η ισχυρή ταυτοποίηση του πελάτη είναι υποχρεωτική για τη διαδικασία δημιουργίας των στοιχείων της άυλης κάρτας εάν η κάρτα εκδίδεται σε διαδικτυακό περιβάλλον. Ως διαδικτυακό περιβάλλον, για τη λειτουργία του οποίου έχει ευθύνη ο ΠΥΠ, στο οποίο διασφαλίζονται η επαρκής ταυτοποίηση του πελάτη και του ΠΥΠ που προσφέρει την υπηρεσία και η προστασία των εμπιστευτικών/ευαίσθητων πληροφοριών, θεωρούνται τα ακόλουθα:

α) οι εγκαταστάσεις του ΠΥΠ,

β) ο δικτυακός τόπος εκτέλεσης τραπεζικών εργασιών μέσω διαδικτύου ή άλλος ασφαλής δικτυακός τόπος, π.χ. στην περίπτωση όπου η αρχή διακυβέρνησης προσφέρει παρόμοια χαρακτηριστικά ασφάλειας, μεταξύ άλλων, όπως αυτά που ορίζονται στο Κεφάλαιο Δ του Τίτλου ΙΙ,

γ) οι υπηρεσίες πληρωμών μέσω αυτόματων ταμειολογιστικών μηχανών, όπου απαιτείται ισχυρή ταυτοποίηση του πελάτη (π.χ. μέσω μικροεπεξεργαστή και προσωπικού κωδικού αναγνώρισης ή μικροεπεξεργαστή και βιομετρικών στοιχείων.

10. Οι ΠΥΠ διασφαλίζουν τη δέουσα διμερή ταυτοποίηση κατά την επικοινωνία τους με επιχειρήσεις ηλεκτρονικού εμπορίου για τους σκοπούς της έναρξης πληρωμών μέσω διαδικτύου και της πρόσβασης σε ευαίσθητα δεδομένα πληρωμών.

Γ. Εγγραφή σε εργαλεία και/ή λογισμικό ταυτοποίησης που παραδίδονται στον πελάτη και παροχή αυτών

1. Οι ΠΥΠ διασφαλίζουν ότι η εγγραφή του πελάτη σε εργαλεία ταυτοποίησης και η αρχική παροχή των εργαλείων αυτών, τα οποία απαιτούνται για τη χρήση της υπηρεσίας πληρωμών μέσω διαδικτύου και/ή η παράδοση λογισμικού σχετικού με τις πληρωμές στους πελάτες διεξάγεται με ασφαλή τρόπο.

2. Η εγγραφή σε εργαλεία ταυτοποίησης και/ή λογισμικό σχετικό με τις πληρωμές που παραδίδονται στον πελάτη και η παροχή αυτών πρέπει να πληρούν τις ακόλουθες προϋποθέσεις:

α) οι σχετικές διαδικασίες διενεργούνται σε ασφαλές και αξιόπιστο περιβάλλον, λαμβανομένων ταυτόχρονα υπόψη των πιθανών κινδύνων που απορρέουν από συσκευές που δεν υπόκεινται στον έλεγχο του ΠΥΠ,

β) εφαρμόζονται αποτελεσματικές και ασφαλείς διαδικασίες για την παράδοση εξατομικευμένων διαπιστευτηρίων ασφάλειας, του λογισμικού που σχετίζεται με τις πληρωμές και όλων των εξατομικευμένων συσκευών που σχετίζονται με τις πληρωμές μέσω διαδικτύου. Το λογισμικό που παραδίδεται μέσω του διαδικτύου πρέπει επίσης να φέρει την ψηφιακή υπογραφή του ΠΥΠ ώστε να παρέχεται η δυνατότητα στον πελάτη να εξακριβώνει τη γνησιότητα αυτού καθώς και ότι αυτό δεν έχει παραποιηθεί,

γ) για συναλλαγές με κάρτα, ο πελάτης έχει την δυνατότητα να εγγραφεί για ισχυρή ταυτοποίηση ανεξαρτήτως μιας συγκεκριμένης αγοράς μέσω διαδικτύου. Στις περιπτώσεις όπου προσφέρεται δυνατότητα ενεργοποίησης στο πλαίσιο αγορών μέσω διαδικτύου, αυτή πραγματοποιείται με ανακατεύθυνση του πελάτη σε ασφαλές και αξιόπιστο περιβάλλον.

3. Για συναλλαγές με κάρτα οι εκδότες ενθαρρύνουν ενεργά την εγγραφή του κατόχου της κάρτας για ισχυρή ταυτοποίηση και επιτρέπουν στους κατόχους κάρτας να παρακάμπτουν την εγγραφή μόνο σε περιορισμένο αριθμό εξαιρετικών περιπτώσεων όπου αυτό δικαιολογείται από τον κίνδυνο που συνδέεται με τη συγκεκριμένη συναλλαγή με κάρτα.

Δ. Απόπειρες σύνδεσης, χρονικό όριο σύνδεσης, διάρκεια ισχύος της ταυτοποίησης

1. Οι ΠΥΠ περιορίζουν τον αριθμό των προσπαθειών σύνδεσης ή ταυτοποίησης, ορίζουν κανόνες για το χρονικό όριο σύνδεσης στις υπηρεσίες πληρωμών μέσω διαδικτύου και θέτουν χρονικά όρια για τη διάρκεια ισχύος της ταυτοποίησης.

2. Όταν χρησιμοποιείται κωδικός αναγνώρισης μίας χρήσης για τους σκοπούς της ταυτοποίησης, οι ΠΥΠ διασφαλίζουν ότι η περίοδος ισχύος των εν λόγω κωδικών αναγνώρισης περιορίζεται αυστηρά στο ελάχιστο αναγκαίο.

3. Οι ΠΥΠ ορίζουν τον μέγιστο αριθμό αποτυχημένων προσπαθειών εισόδου ή ταυτοποίησης, μετά από τον οποίο η πρόσβαση στην υπηρεσία πληρωμών μέσω διαδικτύου αναστέλλεται (προσωρινά ή μόνιμα) και εφαρμόζουν ασφαλή διαδικασία για την εκ νέου ενεργοποίηση των υπηρεσιών πληρωμών μέσω διαδικτύου που έχουν ανασταλεί.

4. Οι ΠΥΠ ορίζουν τη μέγιστη χρονική περίοδο μετά το πέρας της οποίας οι αδρανείς συνδέσεις στις υπηρεσίες πληρωμών μέσω διαδικτύου τερματίζονται αυτομάτως.

Ε. Παρακολούθηση συναλλαγών

1. Οι μηχανισμοί παρακολούθησης των συναλλαγών που έχουν σχεδιαστεί για την πρόληψη, τον εντοπισμό και την προσωρινή άρνηση εκτέλεσης παράνομων πράξεων πληρωμής πρέπει να τίθενται σε λειτουργία πριν από την τελική έγκριση του ΠΥΠ. Οι συναλλαγές που θεωρούνται ύποπτες ή υψηλού κινδύνου πρέπει να υπόκεινται σε ειδική διαδικασία ελέγχου και αξιολόγησης. Ισοδύναμοι μηχανισμοί παρακολούθησης της ασφάλειας και έγκρισης εφαρμόζονται επίσης και για την έκδοση ηλεκτρονικών εξουσιοδοτήσεων.

2. Οι ΠΥΠ χρησιμοποιούν συστήματα ανίχνευσης και πρόληψης της απάτης για τον εντοπισμό ύποπτων συναλλαγών πριν από την τελική έγκριση των πράξεων ή των ηλεκτρονικών εξουσιοδοτήσεων από τον ΠΥΠ. Τα συστήματα αυτά βασίζονται, για παράδειγμα, σε παραμετροποιημένους κανόνες (όπως μαύρες λίστες με στοιχεία καρτών που έχουν διαρρεύσει ή κλαπεί) και παρακολουθούν ασυνήθιστα πρότυπα συμπεριφοράς του πελάτη ή της συσκευής πρόσβασης του πελάτη, όπως τυχόν αλλαγή της διεύθυνσης πρωτοκόλλου ίντερνετ (εφεξής διεύθυνση IP) ή αλλαγή της περιοχής διευθύνσεων IP κατά τη διάρκεια της σύνδεσης στην υπηρεσία πληρωμών μέσω διαδικτύου, η οποία ενίοτε εντοπίζεται μέσω ελέγχων για τον εντοπισμό της γεωγραφικής θέσης της διεύθυνσης IP, ασυνήθεις κατηγορίες επιχειρήσεων ηλεκτρονικού εμπορίου συγκεκριμένου πελάτη ή ασυνήθιστα δεδομένα συναλλαγών. Τα συστήματα αυτά πρέπει επίσης να είναι σε θέση να εντοπίζουν ενδείξεις προσβολής από κακόβουλο λογισμικό κατά τη διάρκεια της σύνδεσης (π.χ. αναγνώριση υποβολής στοιχείων μέσω αυτόματης δέσμης εντολών (script) αντί από

άνθρωπο) καθώς και γνωστών σεναρίων απάτης. Η έκταση, η πολυπλοκότητα και η δυνατότητα προσαρμογής των λύσεων παρακολούθησης είναι ανάλογες με το αποτέλεσμα της αξιολόγησης του κινδύνου και σύμφωνες με τη σχετική νομοθεσία για την προστασία των δεδομένων.

3. Οι ΠΥΠ που αποδέχονται υπηρεσίες συναλλαγών με κάρτα εφαρμόζουν συστήματα εντοπισμού και πρόληψης της απάτης προκειμένου να παρακολουθούν τις δραστηριότητες των επιχειρήσεων ηλεκτρονικού εμπορίου.

4. Οι ΠΥΠ διεξάγουν οποιαδήποτε διαδικασία ελέγχου και αξιολόγησης της συναλλαγής εντός εύλογου χρονικού διαστήματος, προκειμένου να μην καθυστερούν αδικαιολόγητα την έναρξη και/ή την εκτέλεση της σχετικής υπηρεσίας πληρωμής.

5. Στις περιπτώσεις όπου ο ΠΥΠ, σύμφωνα με την πολιτική διαχείρισης κινδύνων που ακολουθεί, αποφασίζει την προσωρινή άρνηση εκτέλεσης μιας πράξης πληρωμής η οποία έχει εντοπιστεί ως πιθανώς παράνομη, ο ΠΥΠ διατηρεί την προσωρινή άρνηση για όσο το δυνατόν συντομότερο χρονικό διάστημα μέχρις ότου επιλυθούν τα ζητήματα ασφάλειας.

ΣΤ. Προστασία των ευαίσθητων δεδομένων πληρωμών

1. Τα ευαίσθητα δεδομένα πληρωμών προστατεύονται κατά την αποθήκευση, την επεξεργασία ή τη διαβίβασή τους, τηρουμένης της ισχύουσας σχετικής νομοθεσίας για την προστασία των προσωπικών δεδομένων.

2. Όλα τα δεδομένα που χρησιμοποιούνται για την αναγνώριση και την ταυτοποίηση των πελατών (π.χ. κατά την είσοδο, κατά την έναρξη πληρωμής μέσω διαδικτύου, καθώς και κατά την έκδοση, τροποποίηση ή ακύρωση ηλεκτρονικών εξουσιοδοτήσεων), όπως επίσης και η διεπαφή του πελάτη (δικτυακός τόπος ΠΥΠ ή επιχείρησης ηλεκτρονικού εμπορίου) προστατεύονται δεόντως από κλοπή, μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση.

3. Οι ΠΥΠ διασφαλίζουν ότι, όταν ανταλλάσσονται ευαίσθητα δεδομένα πληρωμών μέσω του διαδικτύου, εφαρμόζεται ασφαλής διατερματική κρυπτογράφηση, ήτοι η κρυπτογράφηση που πραγματοποιείται εντός ή στο τερματικό σύστημα προέλευσης με την αντίστοιχη αποκρυπτογράφηση να πραγματοποιείται μόνο εντός ή στο τερματικό σύστημα προορισμού, μεταξύ των μερών που επικοινωνούν καθ' όλη τη διάρκεια της σύνδεσης, προκειμένου να διασφαλίζονται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων, με τη χρήση ισχυρών και ευρέως αναγνωρισμένων τεχνικών κρυπτογράφησης.

4. Οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα συστήνουν στις επιχειρήσεις ηλεκτρονικού εμπορίου με τις οποίες συνεργάζονται να μην αποθηκεύουν τυχόν ευαίσθητα δεδομένα πληρωμών. Στην περίπτωση που

επιχειρήσεις ηλεκτρονικού εμπορίου διαχειρίζονται, δηλαδή αποθηκεύουν, επεξεργάζονται ή διαβιβάζουν ευαίσθητα δεδομένα πληρωμών, οι εν λόγω ΠΥΠ πρέπει βάσει σύμβασης να απαιτούν από τις επιχειρήσεις αυτές να εφαρμόζουν τα απαραίτητα μέτρα προστασίας των δεδομένων αυτών. Οι ΠΥΠ διενεργούν τακτικούς ελέγχους και, εάν ένας ΠΥΠ διαπιστώσει ότι επιχείρηση ηλεκτρονικού εμπορίου, η οποία διαχειρίζεται ευαίσθητα δεδομένα πληρωμών, δεν εφαρμόζει τα απαιτούμενα μέτρα ασφάλειας, προβαίνει σε ενέργειες για την επιβολή της συμβατικής αυτής υποχρέωσης ή καταγγέλλει τη σύμβαση.

IV. Ευαισθητοποίηση, εκπαίδευση και επικοινωνία με τους πελάτες

Α. Εκπαίδευση και επικοινωνία με τους πελάτες

1. Οι ΠΥΠ παρέχουν βοήθεια και καθοδήγηση στους πελάτες τους, όπου απαιτείται, όσον αφορά την ασφαλή χρήση των υπηρεσιών πληρωμών μέσω διαδικτύου. Οι ΠΥΠ επικοινωνούν με τους πελάτες τους με τέτοιο τρόπο ώστε να τους διαβεβαιώνουν ως προς τη γνησιότητα των μηνυμάτων που λαμβάνουν.

2. Οι ΠΥΠ παρέχουν τουλάχιστον έναν ασφαλή δίαυλο συνεχούς επικοινωνίας με τους πελάτες σχετικά με την ορθή και ασφαλή χρήση της υπηρεσίας πληρωμών μέσω διαδικτύου (π.χ. με τη χρήση ειδικής ηλεκτρονικής ταχυδρομικής θυρίδας στον δικτυακό τόπο του ΠΥΠ ή ενός ασφαλούς δικτυακού τόπου). Οι ΠΥΠ ενημερώνουν τους πελάτες για τον δίαυλο αυτόν και εξηγούν ότι κάθε μήνυμα που αποστέλλεται εξ ονόματος του ΠΥΠ με οποιοδήποτε άλλο μέσο, όπως με μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο αφορά την ορθή και ασφαλή χρήση της υπηρεσίας πληρωμών μέσω διαδικτύου, δεν είναι αξιόπιστο. Ο ΠΥΠ εξηγεί:

α) τη διαδικασία που πρέπει να ακολουθούν οι πελάτες για να αναφέρουν στον ΠΥΠ υπόνοιες για παράνομες πληρωμές, ύποπτα περιστατικά ή ανωμαλίες κατά τη διάρκεια της σύνδεσης στις υπηρεσίες πληρωμών μέσω του διαδικτύου και/ή πιθανές απόπειρες "κοινωνικής μηχανικής", δηλαδή τεχνικές χειραγώγησης προσώπων για την απόσπαση πληροφοριών (π.χ. μέσω μηνύματος ηλεκτρονικού ταχυδρομείου ή τηλεφωνικών κλήσεων) ή τεχνικές συγκέντρωσης πληροφοριών από μέσα κοινωνικής δικτύωσης, για σκοπούς διάπραξης απάτης ή εξασφάλισης μη εξουσιοδοτημένης πρόσβασης σε υπολογιστή ή δίκτυο.

β) τα επόμενα βήματα, δηλαδή τον τρόπο με τον οποίο ο ΠΥΠ θα απαντήσει στον πελάτη,

γ) τον τρόπο με τον οποίο ο ΠΥΠ θα ενημερώσει τον πελάτη σχετικά με (πιθανές) παράνομες συναλλαγές ή τη αποτυχία έναρξής τους, ή θα προειδοποιήσει τον πελάτη σχετικά με την εκδήλωση επιθέσεων (π.χ. ηλεκτρονικό «ψάρεμα» με μηνύματα ηλεκτρονικού ταχυδρομείου).

3. Μέσω του ασφαλούς διαύλου, ο ΠΥΠ γνωστοποιεί στους πελάτες τις ενημερώσεις των διαδικασιών ασφάλειας όσον αφορά τις υπηρεσίες πληρωμών μέσω διαδικτύου. Τυχόν προειδοποιήσεις σχετικά με σημαντικούς αναδυόμενους κινδύνους (π.χ. προειδοποιήσεις σχετικά με χρήση «κοινωνικής μηχανικής») πρέπει επίσης να παρέχονται μέσω του ασφαλούς διαύλου.

4. Οι ΠΥΠ παρέχουν υπηρεσίες εξυπηρέτησης πελατών αναφορικά με όλα τα ερωτήματα, τα παράπονα, τα αιτήματα υποστήριξης και τις γνωστοποιήσεις για ανωμαλίες ή περιστατικά που αφορούν υπηρεσίες πληρωμών μέσω διαδικτύου και συναφείς υπηρεσίες και ενημερώνουν επαρκώς τους πελάτες σχετικά με τον τρόπο με τον οποίο μπορούν να λάβουν τέτοιου είδους υποστήριξη.

5. Οι ΠΥΠ διοργανώνουν προγράμματα εκπαίδευσης και ευαισθητοποίησης των πελατών προκειμένου να διασφαλίζουν ότι οι πελάτες κατανοούν, τουλάχιστον, την ανάγκη:

α) προστασίας των κωδικών πρόσβασης, των συσκευών παραγωγής πρόσθετου κωδικού ασφάλειας, των προσωπικών στοιχείων και άλλων εμπιστευτικών δεδομένων,

β) ορθής διαχείρισης της ασφάλειας των προσωπικών τους συσκευών (π.χ. του υπολογιστή), μέσω της εγκατάστασης και της ενημέρωσης των στοιχείων ασφάλειας (λογισμικά προστασίας από ιούς, τείχη προστασίας, ενημερώσεις ασφάλειας),

γ) εξέτασης των σημαντικών απειλών και κινδύνων που συνδέονται με τη λήψη λογισμικού μέσω του διαδικτύου, εάν ο πελάτης δεν μπορεί να είναι βέβαιος σε εύλογο βαθμό ότι το λογισμικό είναι γνήσιο και ότι δεν έχει παραποιηθεί,

δ) χρήσης του γνήσιου δικτυακού τόπου πληρωμών μέσω διαδικτύου του ΠΥΠ.

6. Οι ΠΥΠ που αποδέχονται συναλλαγές με κάρτα απαιτούν, βάσει σύμβασης, από επιχειρήσεις ηλεκτρονικού εμπορίου το σαφή διαχωρισμό της διαδικασίας πληρωμής από το περιβάλλον του ηλεκτρονικού καταστήματος προκειμένου να καθίσταται κατανοητό στους πελάτες ότι η συναλλαγή πραγματοποιείται με τον ΠΥΠ και όχι με τον δικαιούχο πληρωμής (π.χ. με ανακατεύθυνση του πελάτη και άνοιγμα χωριστού παραθύρου ώστε η διαδικασία πληρωμής να μην εμφανίζεται σε ένα πλαίσιο εντός της ιστοσελίδας της επιχείρησης ηλεκτρονικού εμπορίου).

Β. Ειδοποιήσεις, καθορισμός ορίων

1. Οι ΠΥΠ σύμφωνα με τα οριζόμενα στην παρ. 1 του άρθρου 52 του Ν. 3862/2010 δύνανται να συμφωνούν με τους πληρωτές όρια δαπανών για τις υπηρεσίες πληρωμών μέσω διαδικτύου και παρέχουν δυνάμει σχετικού συμβατικού όρου στους πελάτες τους επιλογές για περαιτέρω περιορισμό του κινδύνου εντός των ορίων

αυτών. Μπορούν επίσης να παρέχουν υπηρεσίες προειδοποίησης και διαχείρισης του προφίλ πελατών.

2. Πριν από την παροχή υπηρεσιών πληρωμών μέσω διαδικτύου σε πελάτες, οι ΠΥΠ θέτουν όρια με ισχύ είτε μεμονωμένη είτε καθολική (δηλαδή για όλα τα μέσα πληρωμής που παρέχουν δυνατότητα πληρωμών μέσω διαδικτύου) που θα ισχύουν για τις υπηρεσίες αυτές (π.χ. μέγιστο ποσό για κάθε επιμέρους πληρωμή ή συγκεντρωτικό ποσό για πληρωμές που διενεργούνται εντός μιας συγκεκριμένης χρονικής περιόδου) και ενημερώνουν σχετικά τους πελάτες τους. Οι ΠΥΠ παρέχουν στους πελάτες τη δυνατότητα απενεργοποίησης της λειτουργίας πληρωμής μέσω διαδικτύου.

Γ. Πρόσβαση των πελατών σε πληροφορίες σχετικά με την κατάσταση έναρξης και εκτέλεσης της πληρωμής

1. Οι ΠΥΠ επιβεβαιώνουν στους πελάτες τους την έναρξη της πληρωμής και τους παρέχουν εγκαίρως τις απαραίτητες πληροφορίες ώστε να ελέγχουν την ορθή έναρξη και/ή εκτέλεση της πράξης πληρωμής.

2. Οι ΠΥΠ προκειμένου για τη διενέργεια των υπηρεσιών της μεταφοράς πίστωσης ή/και της ηλεκτρονικής εξουσιοδότησης, παρέχουν στους πελάτες τη δυνατότητα να ελέγχουν την κατάσταση της εκτέλεσης των πράξεων σε σχεδόν πραγματικό χρόνο, καθώς και τα υπόλοιπα λογαριασμών ανά πάσα στιγμή σε ένα ασφαλές και αξιόπιστο περιβάλλον εκτός από τις έκτακτες περιπτώσεις μη διαθεσιμότητας της υπηρεσίας αυτής για λόγους τεχνικής συντήρησης, ή λόγω σοβαρών περιστατικών.

3. Οποιοδήποτε λεπτομερές ηλεκτρονικό παραστατικό καθίσταται διαθέσιμο σε ασφαλές και αξιόπιστο περιβάλλον. Όταν οι ΠΥΠ ενημερώνουν τους πελάτες σχετικά με τη διαθεσιμότητα ηλεκτρονικών παραστατικών (π.χ. ανά τακτά χρονικά διαστήματα, όταν εκδίδεται περιοδικό ηλεκτρονικό αντίγραφο κίνησης λογαριασμού, ή κατά περίπτωση μετά την εκτέλεση μιας πράξης) μέσω εναλλακτικού διαύλου, όπως μέσω γραπτού μηνύματος (SMS), μηνύματος ηλεκτρονικού ταχυδρομείου ή επιστολής, τα ευαίσθητα δεδομένα πληρωμής είτε δεν περιλαμβάνονται στην επικοινωνία αυτή είτε, εφόσον περιλαμβάνονται, εμφανίζονται συγκαλυμμένα.

V. Τελικές διατάξεις

1. Συστήνεται στα ΠΥΠ να ακολουθούν στις πολιτικές που θεσπίζουν για την ασφάλεια πληρωμών μέσω διαδικτύου τις βέλτιστες πρακτικές που αναφέρονται στο Παράρτημα της παρούσας.

2. Οι διατάξεις της παρούσας ισχύουν από την ημερομηνία δημοσίευσής της στην Εφημερίδα της Κυβερνήσεως.

Η ΕΚΤΕΛΕΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

3. Εξουσιοδοτείται η Διεύθυνση Εποπτείας Εποπτευόμενων Εταιρειών της Τράπεζας της Ελλάδος για την παροχή των τυχόν αναγκαίων διευκρινίσεων και οδηγιών για την εφαρμογή της παρούσας.

4. Η παρούσα να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως και να αναρτηθεί στον ιστότοπο της Τράπεζας της Ελλάδος.

Ο Υποδιοικητής	Ο Υποδιοικητής	Ο Διοικητής
Θεόδωρος Μητράκος	Ιωάννης Μουρμούρας	Ιωάννης Στουρνάρας

Ακριβές Αντίγραφο,
Αθήνα, 15/2/16
Διεύθυνση Εποπτείας Πιστωτικού Συστήματος
Η Διευθύντρια

Σ. Παπαγιαννίδου

ΠΑΡΑΡΤΗΜΑ

Βέλτιστες πρακτικές (ΒΠ) για την ασφάλεια πληρωμών μέσω διαδικτύου

Γενικό περιβάλλον ελέγχου και ασφάλειας (σχετ. Τίτλος ΙΙ):

- **Διακυβέρνηση (σχετ. Κεφάλαιο Α)**

ΒΠ 1: Η πολιτική ασφάλειας μπορεί να καταγράφεται σε ειδικό έγγραφο.

- **Έλεγχος και μείωση των κινδύνων (σχετ. Κεφάλαιο Δ)**

ΒΠ 2: Οι ΠΥΠ μπορούν να παρέχουν εργαλεία ασφάλειας (π.χ. συσκευές ή/και ειδικά προσαρμοσμένα προγράμματα περιήγησης, που προστατεύονται δεόντως) για την προστασία της διεπαφής με τον πελάτη από παράνομη χρήση ή επιθέσεις (π.χ. επιθέσεις τύπου «man in the browser»).

- **Ιχνηλασιμότητα**

ΒΠ 3: Οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα μπορούν να απαιτούν βάσει σύμβασης από τις επιχειρήσεις ηλεκτρονικού εμπορίου που αποθηκεύουν πληροφορίες σχετικά με πληρωμές να εφαρμόζουν επαρκείς διαδικασίες για την υποστήριξη της ιχνηλασιμότητας.

Ειδικά μέτρα ελέγχου και ασφάλειας για τις πληρωμές μέσω διαδικτύου (σχετ. Τίτλος ΙΙΙ):

- **Αρχική εξακρίβωση ταυτότητας πελάτη, ενημέρωση (σχετ. Κεφάλαιο Α)**

ΒΠ 4: Ο πελάτης μπορεί να συνάπτει ειδική σύμβαση παροχής υπηρεσιών για την εκτέλεση πράξεων πληρωμής μέσω διαδικτύου, αντί να περιλαμβάνονται οι όροι για τις υπηρεσίες αυτές σε ευρύτερη σύμβαση παροχής γενικών υπηρεσιών που συνάπτεται με τον ΠΥΠ.

ΒΠ 5: Οι ΠΥΠ μπορούν επίσης να μεριμνούν για την παροχή στους πελάτες, σε συνεχή βάση ή, όπου εφαρμόζεται, κατά περίπτωση και με κατάλληλα μέσα (π.χ. φυλλάδια, ιστοσελίδες), σαφών και κατανοητών οδηγιών στο πλαίσιο των οποίων επεξηγούνται οι ευθύνες τους για την ασφαλή χρήση της υπηρεσίας.

- **Ισχυρή ταυτοποίηση του πελάτη (σχετ. Κεφάλαιο Β)**

ΒΠ 6: Για τις πράξεις πληρωμών με κάρτα οι επιχειρήσεις ηλεκτρονικού εμπορίου μπορούν να υποστηρίζουν την ισχυρή ταυτοποίηση του κατόχου της κάρτας από τον εκδότη σε συναλλαγές με κάρτα μέσω του διαδικτύου.

ΒΠ 7: Για τους σκοπούς της διευκόλυνσης των πελατών, οι ΠΥΠ μπορούν να εξετάσουν το ενδεχόμενο χρήσης ενός ενιαίου εργαλείου ισχυρής ταυτοποίησης του πελάτη για όλες τις υπηρεσίες πληρωμών μέσω διαδικτύου. Αυτό θα μπορούσε να αυξήσει την αποδοχή της λύσης από τους πελάτες και να διευκολύνει την ορθή χρήση.

ΒΠ 8: Η ισχυρή ταυτοποίηση του πελάτη μπορεί να περιλαμβάνει στοιχεία που συνδέουν την ταυτοποίηση με ένα συγκεκριμένο ποσό και έναν συγκεκριμένο δικαιούχο πληρωμής. Αυτό θα μπορούσε να παράσχει στους πελάτες αυξημένη βεβαιότητα κατά την έγκριση πληρωμών. Η τεχνολογική λύση που διευκολύνει τη σύνδεση των δεδομένων ισχυρής ταυτοποίησης με τα δεδομένα των συναλλαγών πρέπει να είναι ανθεκτική στην παραποίηση.

- **Προστασία των ευαίσθητων δεδομένων πληρωμών (σχετ. Κεφάλαιο ΣΤ)**

ΒΠ 9: Είναι επιθυμητό οι επιχειρήσεις ηλεκτρονικού εμπορίου που χειρίζονται ευαίσθητα δεδομένα πληρωμών να εκπαιδεύουν καταλλήλως το προσωπικό τους που είναι αρμόδιο για τη διαχείριση περιστατικών απάτης και να επικαιροποιούν την εκπαίδευση αυτή τακτικά, ώστε να διασφαλίζεται ότι το περιεχόμενό της ανταποκρίνεται σε ένα δυναμικό περιβάλλον ασφάλειας.

<u>Ευαισθητοποίηση, εκπαίδευση και επικοινωνία με τους πελάτες (σχετ. Τίτλος IV):</u>

- **Εκπαίδευση και επικοινωνία με τους πελάτες (σχετ. Κεφάλαιο Α)**

ΒΠ 10: Είναι επιθυμητό οι ΠΥΠ που προσφέρουν υπηρεσίες αποδοχής συναλλαγών με κάρτα να διοργανώνουν εκπαιδευτικά προγράμματα προς τις συνεργαζόμενες επιχειρήσεις ηλεκτρονικού εμπορίου σχετικά με την πρόληψη της απάτης.

- **Ειδοποιήσεις, καθορισμός ορίων (σχετ. Κεφάλαιο Β)**

ΒΠ 11: Στο πλαίσιο των καθορισμένων ορίων δαπανών, οι ΠΥΠ μπορούν να παρέχουν στους πελάτες τους τη δυνατότητα να διαχειρίζονται τα όρια δαπανών των υπηρεσιών πληρωμών μέσω διαδικτύου σε ένα ασφαλές και αξιόπιστο περιβάλλον.

ΒΠ 12: Οι ΠΥΠ μπορούν να εφαρμόζουν διαδικασίες προειδοποίησης των πελατών, όπως μέσω τηλεφωνικής επικοινωνίας ή αποστολής γραπτού μηνύματος (SMS), για ύποπτες ή υψηλού κινδύνου πράξεις πληρωμών που βασίζονται στις εσωτερικές τους πολιτικές για τη διαχείριση κινδύνων.

ΒΠ 13: Οι ΠΥΠ μπορούν να παρέχουν στους πελάτες τη δυνατότητα να προσδιορίζουν γενικούς, εξατομικευμένους κανόνες ως παραμέτρους για τη συμπεριφορά τους όσον αφορά τις πληρωμές μέσω διαδικτύου και τις συναφείς υπηρεσίες (π.χ. ότι οι πελάτες μπορούν να δρομολογούν πληρωμές μόνο από κάποιες συγκεκριμένες χώρες και ότι οι πληρωμές που δρομολογούνται από άλλα σημεία θα τίθενται σε προσωρινή άρνηση, ή ότι μπορούν να συμπεριλαμβάνουν συγκεκριμένους δικαιούχους πληρωμής σε λευκές ή μαύρες λίστες).