



Ασφάλεια Εναλλακτικών Δικτύων

Κωνσταντίνος Μαρινάκης



ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ

Περιεχόμενα παρουσίασης



1

Εναλλακτικά δίκτυα

2

Κίνδυνοι

3

Μορφές και οργάνωση e-Fraud

4

e-Fraud Life Cycle

5

Ενιαία αντιμετώπιση

6

Προτεινόμενα μέτρα

Εξέλιξη εναλλακτικών δικτύων

Δίκτυα Εξέλιξη με κινδύνους

Αρχική μορφή

- Μικρά δίκτυα με dedicated κλειστές γραμμές επικοινωνίας.
- Ασφαλή λειτουργικά συστήματα
- Έλεγχος ασφάλειας στα χέρια της Τράπεζας

Παρούσα μορφή

- Εκτεταμένα δίκτυα με ανοικτές πλατφόρμες και επικοινωνιακές υποδομές.
- Νέα δίκτυα - νέες τεχνολογίες (ασύρματα, δορυφορικά).
- Μέρος της ασφάλειας στα χέρια του πελάτη

Κίνδυνοι e-Fraud

Λειτουργικός Κίνδυνος

Κίνδυνος Απώλειας Φήμης

Κανονιστική Συμμόρφωση

**Απώλεια
χρημάτων, φήμης,
πελατείας.
Ενδεχόμενα
πρόστιμα.**

Μέθοδοι e-Fraud

1

ATMs

- Κλοπή κάρτας & Pin
- Card trapping
- Cash trapping
- Skimming *
- Physical attack

2

Internet Banking

- Phishing (e-mail)
- Spoofing
- Pharming
- Man in the middle
- ...

3

Άλλα κανάλια

- Phishing (phone)
- Identity theft (mail)
- Social Engineering
- ...

Μέθοδοι e-Fraud

4

Phishing με e-mail

Skimming σε ATM ή POS

- ▶ Αναλήψεις από ATM
- ▶ Χρεώσεις μέσω POS ή Internet

- Οι απατεώνες επιλέγουν κάθε φορά τον προσφορότερο τρόπο υποκλοπής και χρήσης των κωδικών
- Δύσκολος εντοπισμός εάν δεν υπάρχει συντονισμός ανάμεσα στην παρακολούθηση όλων των εναλλακτικών δικτύων

Μέθοδοι e-Fraud - Εξέλιξη

❖ Οι μέθοδοι e-Fraud εξελίσσονται με την τεχνολογία



e-Fraud: Οργανωμένο έγκλημα

❖ Οργανωμένες σπείρες υπό κεντρική καθοδήγηση



Π.χ. Οι μηχανισμοί skimming
έρχονται στην Ελλάδα από Ιταλία

Ενώ ο αρχικός και
τελικός έλεγχος
γίνεται από τη
Ρουμανία

Στις σπείρες
συμμετέχουν αρκετά
άτομα από τη
Βουλγαρία

Κύκλος Ζωής e-Fraud (Fraud Life Cycle)

- ❖ Όπως σε όλες τις τεχνολογίες έτσι και στις μεθόδους fraud παρατηρούμε τα κλασικά στάδια ενός κύκλου ζωής

Πρωλειών από Fraud

Εισαγωγή

Ανάπτυξη

Ωρίμανση

Παρακμή

Στάδιο Εισαγωγής

- Δοκιμαστική χρήση επιλεγμένα σημεία
- Σε εξέλιξη η μέθοδος ο εξοπλισμός
- Εξακρίβωση & της μεθόδου.

Στάδιο Ανάπτυξης

- Επιλογή σε χώρες & περιοχές με υψηλότερα περιθώρια απόδοσης.
- Αύξηση περιστατικών.
- Βελτίωση των μεθόδων
- Εκμετάλλευση των κενών που εντοπίστηκαν κατά το στάδιο της εισαγωγής.

Στάδιο Ωρίμανσης

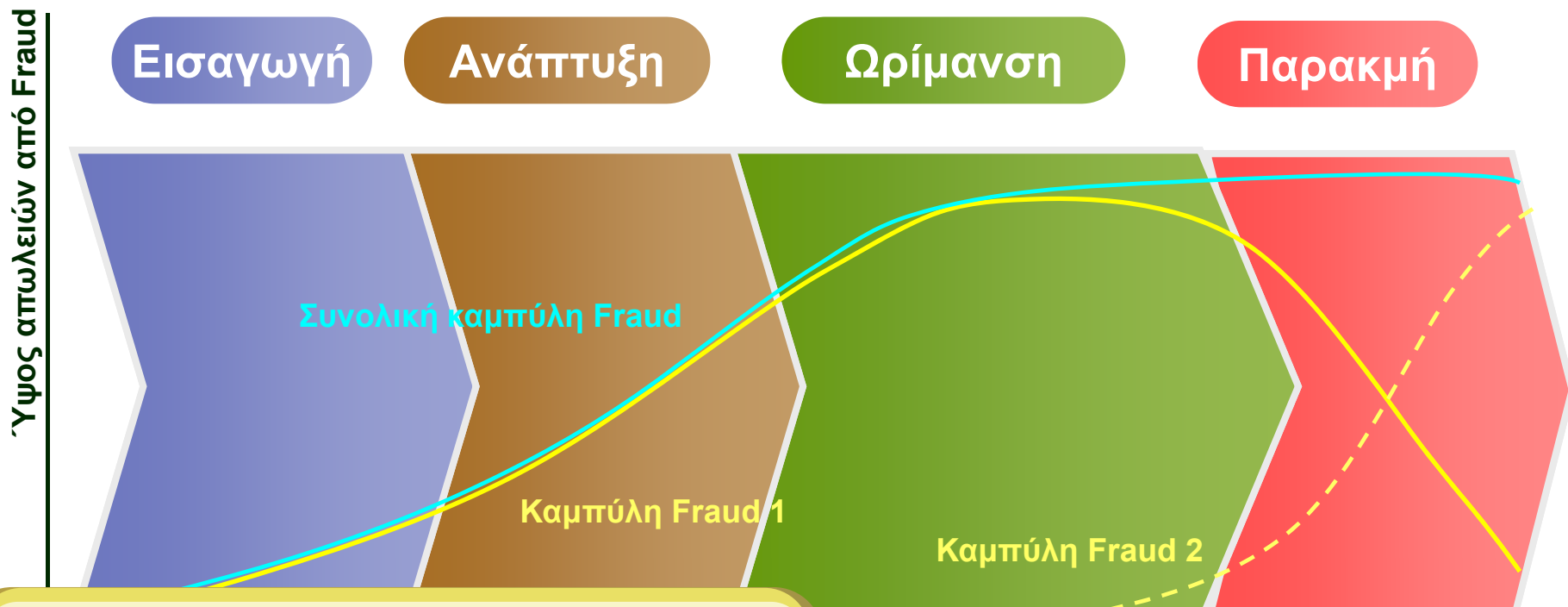
περισσότερα και σε
πυρην
ση σε
να ευ
θε Τρο

Στάδιο παρακμής

- Υιοθέτηση αποτελεσματικών μέτρων anti-fraud

Κύκλος Ζωής e-Fraud (Fraud Life Cycle)

- ❖ Ανάπτυξη & εισαγωγή νέων πιο αποτελεσματικών μεθόδων Fraud



Αύξηση των απωλειών από fraud λόγω αποτελεσματικότητας της νέας μεθόδου. Οι συνολικές απώλειες είναι το άθροισμα των απωλειών των δύο διαφορετικών μεθόδων.

Εάν δεν έχει βρεθεί τρόπος αντιμετώπισης, οι απατεώνες ενδέχεται να χρησιμοποιήσουν εκ νέου την παλαιά μέθοδο.

Κύκλος Ζωής e-Fraud (Fraud Life Cycle)

- ❖ Υιοθέτηση αποτελεσματικών μέτρων anti-fraud από τις Τράπεζες

Πωλειών από Fraud

Εισαγωγή

Ανάπτυξη

Ωρίμανση

Παρακμή

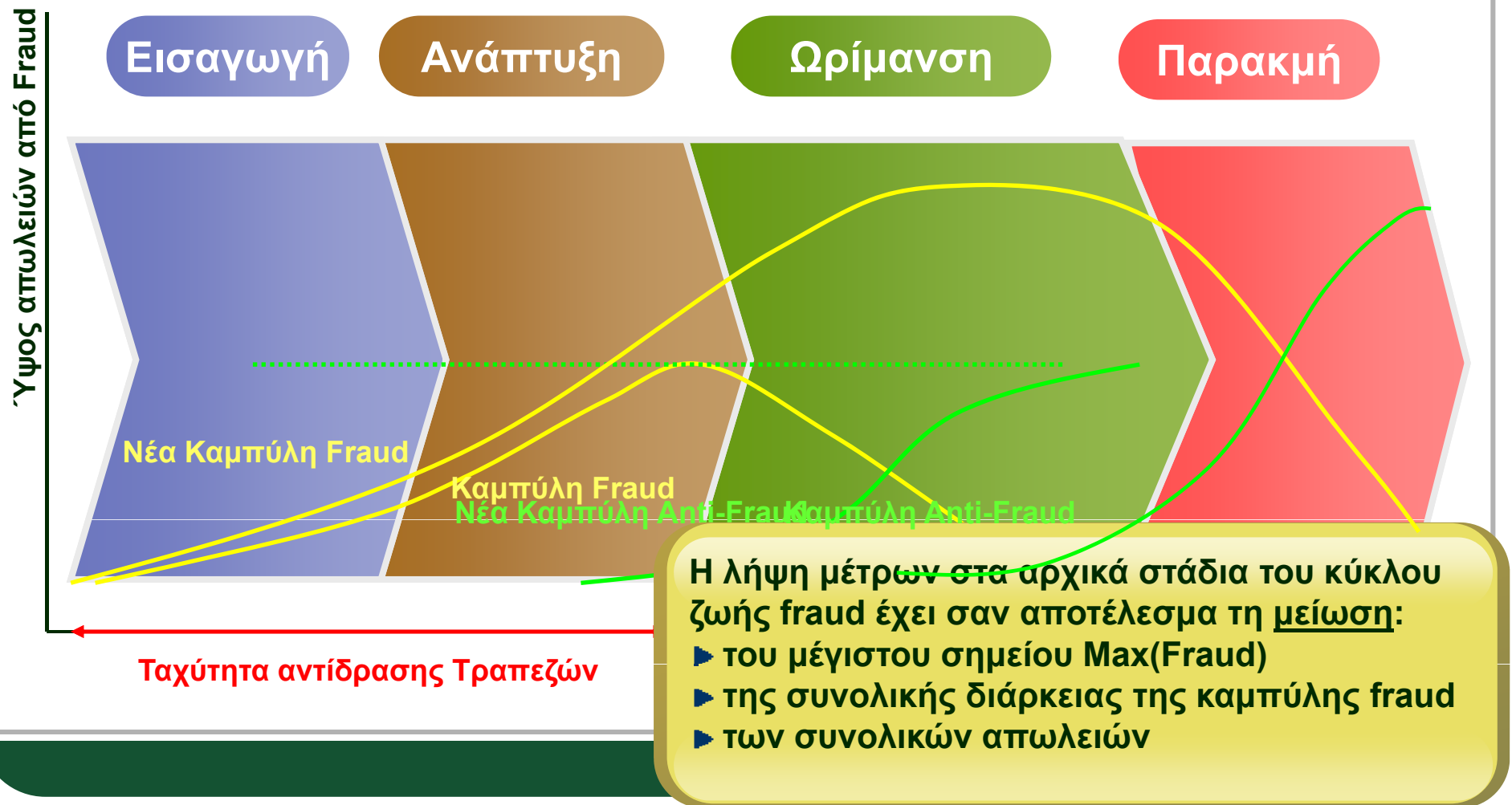
Σε άριστη περίπτωση τα μέτρα θα πρέπει να είναι σε θέση να εξουδετερώνουν πλήρως όλες τις προσπάθειες απάτης.

$$\text{Max(Anti-Fraud)} = \text{Max(Fraud)}$$

Εξειδικευμένα μέτρα δεν μπορούν να ανταποκριθούν σε διαφοροποιήσεις των μεθόδων fraud.
π.χ. μηχανισμός anti-skimming που έχει κατασκευαστεί ειδικά για έναν τύπο ATM, δεν μπορεί να χρησιμοποιηθεί σ' άλλον.

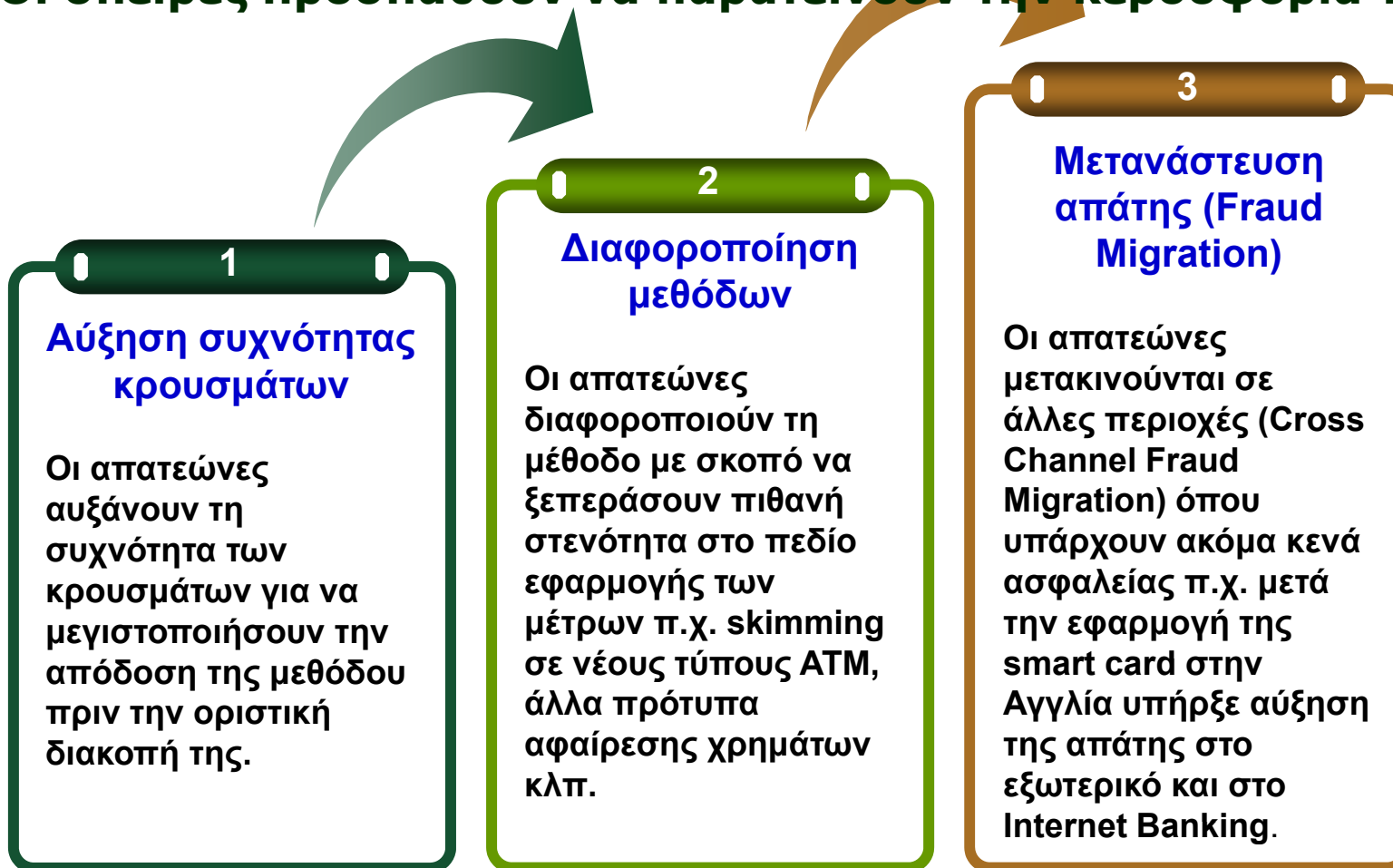
Κύκλος Ζωής e-Fraud (Fraud Life Cycle)

- ❖ Υιοθέτηση αποτελεσματικών μέτρων anti-fraud από τις Τράπεζες



Αντίδραση fraudsters στα μέτρα anti-fraud

- ❖ Οι σπείρες προσπαθούν να παρατείνουν την κερδοφορία τους



Η αντιμετώπιση απαιτεί γνώση

Περιστατικά
e-fraud

Συλλογή, επεξεργασία και ανάλυση στοιχείων

Μέθοδοι και
κύκλος ζωής
e-fraud

Profil
Τράπεζας
ή χώρας

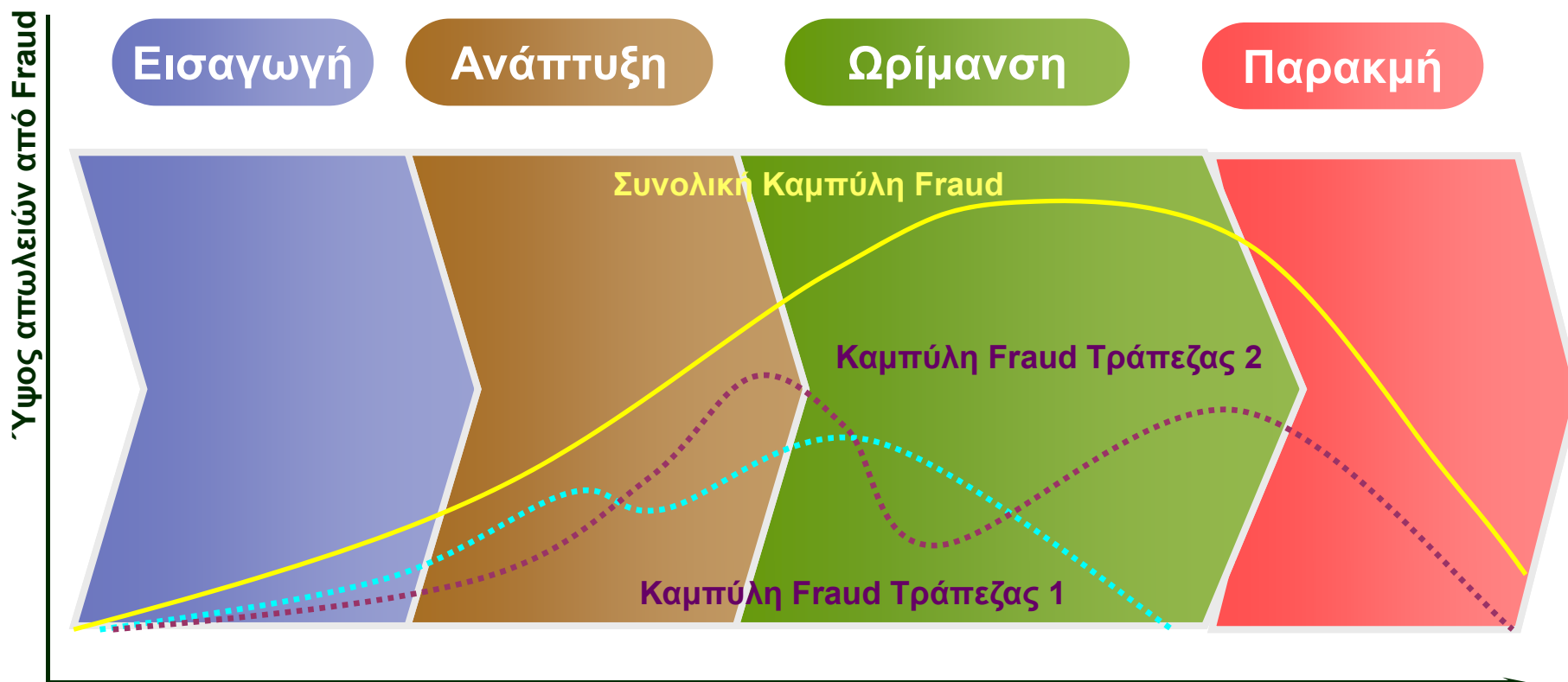
Ορισμός
βασικών
δεικτών (ΚΙ)

Εκτίμηση
αποτελεσμα-
τικότητας
Anti-Fraud

Αποτελεσματική αντιμετώπιση Fraud

Αντιμετώπιση e-Fraud ανά ίδρυμα

- ❖ Κάθε Τράπεζα αντιμετωπίζει διαφορετική καμπύλη Fraud η οποία εξαρτάται από το profil της αλλά και από τη συγκυρία



Αντιμετώπιση e-Fraud ανά ίδρυμα

- ❖ Κάθε Τράπεζα αντιμετωπίζει διαφορετική καμπύλη Fraud η οποία εξαρτάται από το profil της αλλά και από τη συγκυρία

Ύψος απωλειών από Fraud

Εισαγωγή

Ανάπτυξη

Ωρίμανση

Παρακμή

Συνολική Καμπύλη Fraud

Η ελλιπής γνώση οδηγεί σε σπατάλη πόρων και σε αναποτελεσματικές λύσεις

και έντασης από την αντίστοιχη καμπύλη της Τράπεζας 2.

Καμπύλη Fraud Τράπεζας 2

Ωστόσο οι καμπύλες και των δύο Τραπεζών δεν αντικατοπτρίζουν το συνολικό ύψος των απωλειών λόγω fraud, το οποίο είναι κατά πολύ μεγαλύτερο.

Καμπύλη Fraud Τράπεζας 1

Σαν αποτέλεσμα οι Τράπεζες ενδέχεται να υποτιμήσουν το μέγεθος της απειλής.

Ενιαία αντιμετώπιση e-fraud

Απαραίτητη η συνεργασία σε ενδοτραπεζικό, διατραπεζικό και διεθνές επίπεδο μεταξύ Τραπεζών, διωκτικών αρχών και άλλων φορέων

Συλλογή στοιχείων

Συλλογή δεδομένων από όλα τα εναλλακτικά δίκτυα των μελών

Ανατροφοδότηση

Εκτίμηση του αποτελέσματος και ανατροφοδότηση του συστήματος συλλογής δεδομένων

μέτρων

Αξιολόγηση



Εφαρμογή των καταλληλότερων μέτρων

Εφ

Ανάλυση

- Ανάλυση στοιχείων
- Εντοπισμός απειλών και πιθανών τρόπων αντιμετώπισης,
- Καθορισμός και παρακολούθηση Κ.Ι.

Ενιαία αντιμετώπιση e-fraud

Αποτελέσματα ενιαίας αντιμετώπισης

- Σχηματισμός πλήρους εικόνας για πιθανές απειλές
- Άμεση πληροφόρηση - μείωση του χρόνου λήψης μέτρων
- Ανίχνευση fraud migration
- Αντιμετώπιση πολύπλοκων, υβριδικών μορφών απάτης
- Καλλίτερη συνεργασία με άλλα ιδρύματα του εξωτερικού και διωκτικές αρχές

Αποτελέσματα αποτυχίας ενιαίας αντιμετώπισης

- Αποσπασματική πληροφόρηση
- Πλαστή αίσθηση ασφάλειας
- Αυξημένος χρόνος αντίδρασης
- Ανεπαρκής γνώση fraud patterns
- Χρονοβόρα συνεργασία με άλλες Τράπεζες και Οργανισμούς
- Αύξηση κόστους fraud:
 - ▶ Αύξηση ζημιών
 - ▶ Αύξηση κεφαλαιακών απαιτήσεων
 - ▶ Αύξηση κόστους προσωπικού
 - ▶ Δέσμευση πόρων σε μη αποτελεσματικά μέτρα

Το παράδειγμα της Αγγλίας

Επιπρόσθετα η APACS ανακοίνωσε τη δημιουργία του FISS (Fraud Intelligence Sharing System) με σκοπό την ανταλλαγή πληροφοριών για κάθε κρούσμα απάτης μέσω μιας κεντρικής κοινόχρηστης βάσης δεδομένων.

Το 2008 το FIB (Fraud Intelligence Bureau) του Τραπεζικού Τομέα που ήταν υπεύθυνο για την ανταλλαγή στοιχείων μεταξύ των Τραπεζών και των διωκτικών αρχών, σε συνεργασία με το γραφείο πληροφοριών του DCPCU, ίδρυσαν την PIPJIU (Payment Industry & Police Joint Intelligence Unit)

Η APACS (Association for Payment) + Metropolitan Police + Δήμος Λονδίνου = DCPCU (Dedicated Cheque & Plastic Crime)

APACS

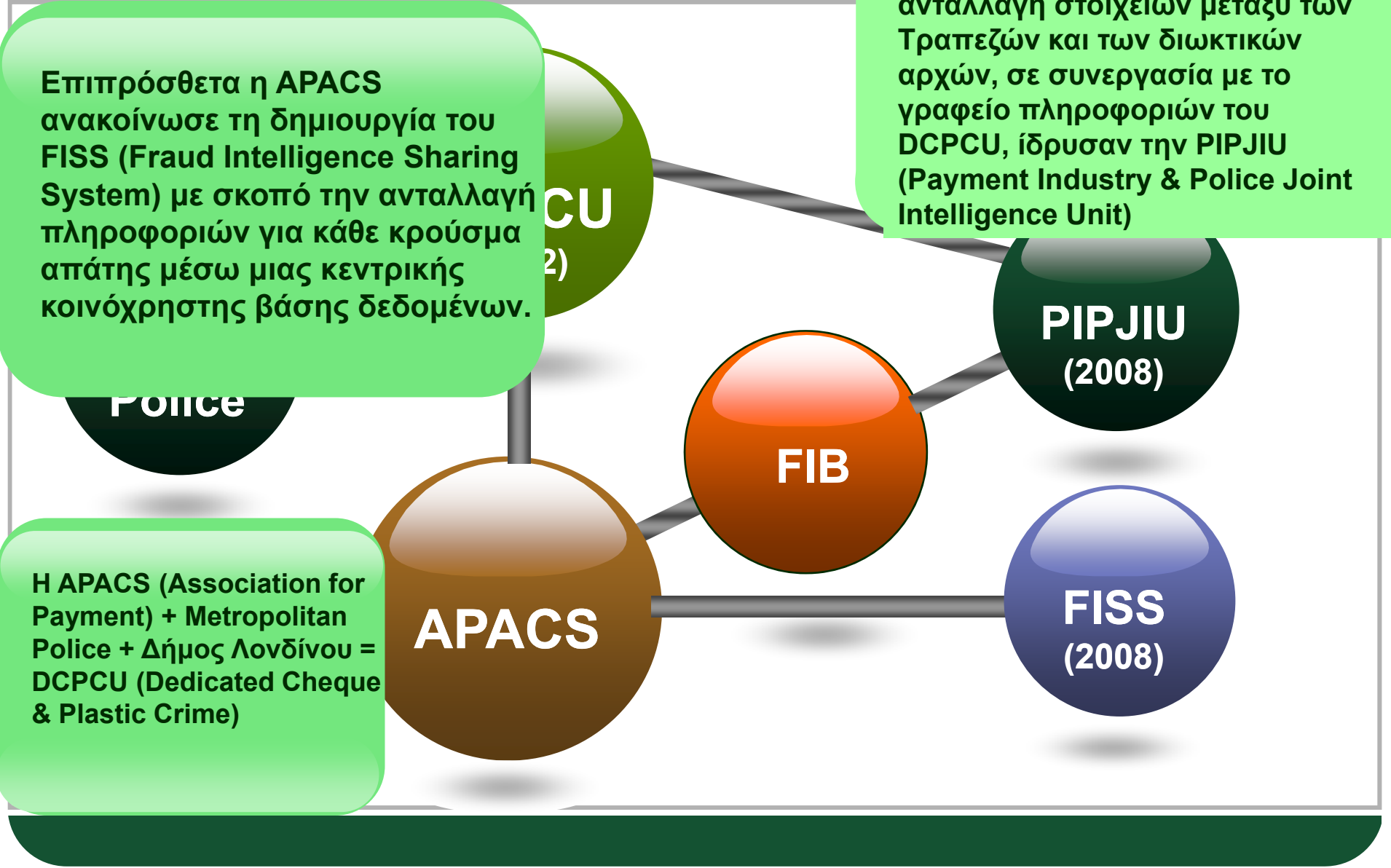
FIB

PIPJIU
(2008)

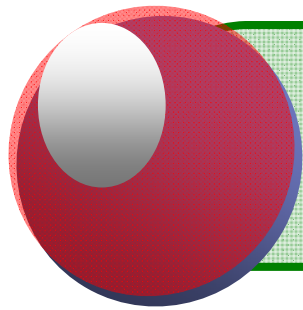
FISS
(2008)

Police

DCPCU
(2)



Πρόταση



**Δημιουργία Μονάδας Αντιμετώπισης
Ηλεκτρονικής Απάτης στην ΕΕΤ**

Οργάνωση – Μεθοδολογία - Συστήματα

1

Δημιουργία κοινόχρηστης βάσης δεδομένων fraud με πρόσβαση για τα μέλη που θα περιλαμβάνει μεθόδους και πρότυπα fraud, ύποπτες κάρτες και άλλα στοιχεία

2

Συνεργασία με τις διωκτικές αρχές και Πανεπιστημιακά Ιδρύματα για ανάλυση των στοιχείων, καθορισμό profil και βασικών δεικτών των ελληνικών Τραπεζών

3

Συνεχής αναβάθμιση των συστημάτων παρακολούθησης & πρόληψης των Τραπεζών για τα Εναλλακτικά Δίκτυα



Ευχαριστώ για τη προσοχή σας

Κωνσταντίνος Μαρινάκης



ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ