Aider les émetteurs à protéger les données

Mastercard Early Detection System

LE "BUSINESS" DES DONNÉES VOLÉES EST :

+400%

EN FORTE CROISSANCE

Taux de fraudes sur les smartphones et l'IoT[1]

4.2B

CONSIDÉRABLE

donées volées en 2016[2]

9 minutes

PLUS RAPIDE

le temps pour publier sur le dark web des données volées[3]

CARACTÉRISTIQUES DE LA PLUPART DES OUTILS POUR STOPPER LA FRAUDE APRES LE VOL DE DONNÉES :

40%

REACTIVTÉ

des consommateurs utilisent rarement leur carte de remplacement, uniquement dans certaines situations [4]

95%-97%

ÉTENDUE

des numéros de cartes identifiées par ADC ne subissent pas de fraudes [5]

6-18 mois

LENTEUR

entre le moment de la fraude et l'alerte aux émetteurs[5]

MASTERCARD FOURNIT AUX ÉMETTEURS DES INFORMATIONS CIBLÉES ET PRIORISÉES SUR LE RISQUE DE FRAUDE* A L'AIDE DE DONNÉES PROPRIÉTAIRES, DE LA MODÉLISATION ET DE LA VISIBILITÉ DE NOTRE RÉSEAU MONDIAL AVANT QUE LA FRAUDE N'AIT LIEU

Aide à réduire la fraude et les coûts annexes grâce à une surveillance accrues des comptes à risque*

Protège la fidélité des titulaires de cartes et diminue l'attrition grâce à la détection précoce de la fraude et une réémission informelle des cartes

*Les niveaux de confiance indiquent la probabilité pour que le numéro des cartes identifiées soit utilisé à des fins de fraude. La fraude peut toutefois ne pas se produire

Avec Early Detection System, les émetteurs peuvent prendre des mesures proactives pour diminuer le taux de fraude. Sa seule installation suffit.

Pour plus d'informations sur Mastercard Early Detection System, rendez-vous sur :

newsroom.mastercard.com

SOURCES :
1. Nokia threat intelligence report- 2H 2016. 2017.
2. Risk Based Security. Annual Data Breach Quick View Report. 2017.
3. FTC. GOV. How fast will identity thieves use stolen info? May 2017.
4. ABA. Target Breach Impact Survey. 2014.
5. Mastercard Data Warehouse. 2017.