# 防制支付詐欺

NetGuardians

**隨著行動 / 電子支付、開放銀行與數位互動交易的普遍，**
**詐欺手法層出不窮，傳統的防制支付詐欺已無法有效的防止詐欺發生，**
**還會加重銀行潛在的責任負擔。**


大多數傳統防制支付詐欺系統依靠對已知的詐欺案例進行分析，但是無法偵測新的交易詐欺行為模式，且易產生大量誤報，降低營運效率與客戶體驗滿意度。這對於想要對交易詐欺進行快速與精準防制的銀行，顯然是不夠的。另外，身份認證的方法也不夠完善，也會被詐欺者加以利用。

NetGuardians的平台NG | Screener可以即時分析銀行所有支付交易，透過屢獲殊榮的NG 3D AI人工智慧科技，準確檢測更多詐欺案例並降低誤報率；可以偵測到來自於社交工程攻擊（如：發票詐騙、戀愛詐騙、CEO詐騙），或是網路詐騙的可疑交易（如：被惡意軟體重新導向的交易連線、被惡意劫持的交易連線、身份盜用）。

## 在支付詐欺發生之前阻止

NetGuardians的防制支付詐欺解決方案提供即時、預先定義的AI風險模組，應用於即時檢測詐欺交易。可以確保符合SWIFT CSP與PSD2規範要求，同時主動找當前及未來出現的支付詐欺手法，此系統可彈性部署於地端或雲端。

**不同於傳統以規則為基礎的防制支付詐欺系統**

**使用NG | Screener可以做到：**

- → **減少誤報率最高達85%**
- → **降低營運成本75%**
- → **事件調查時間縮短高達93%**

### 免除資料蒐集困擾：

NG | Screener 運用連接器介接直接讀取、檢測並分析交易資料，從第一天起便可以發現並阻止支付詐欺。

### 即時檢測的人工智慧科技(3D AI)風險模組：

NG | Screener的人工智慧科技(3D AI)風險模組負責所有繁重的任務。透過對交易變量參數的監測，即時發現並標記出任何支付交易裡的異常。

### 可解釋性人工智慧科技(3D AI)：

你不需要專業人員來對報告進行分析，一個簡單的儀表板報表可以讓您輕鬆一目瞭然事件警示發生原因，並提供即時事件前後關係的完整背景資訊；透過強大的圖表解析工具，讓調查方便直觀。

## 使用案例

- 發票詐騙
- 社交工程
- 詐騙（戀愛詐騙、CEO詐騙）
- SWIFT網絡詐欺
- 被惡意軟體重新導向的數位銀行交易
- 被惡意劫持的數位銀行交易連線
- SIM卡交換
- 網路釣魚造成身份盜用
- 偽造行動銀行APP

### 屢獲肯定：

GARTNER 2020年網路詐欺防制市場指引

CHARTIS 2021年企業詐欺報告

AITE 2021年詐欺&反洗錢機器學習平台報告

更多產品資訊洽詢

BAOYI / 寶誼資訊股份有限公司

02-2308-7700 | sales@baoyi-info.com.tw | https://www.baoyi-info.com.tw