FraudNet

強大的詐欺檢測和流暢的客戶體驗。
您是否能同時擁有？

要抓住罪犯，就要像罪犯那樣思考。FraudNet 的設計初衷就是讓詐欺更為困難，讓客戶體驗更加流暢。FraudNet 的多層決策分析方法可針對可疑事件和共同特徵做出明智的決定，並在後台進行關聯分析，使您快速辨識出具備共同特徵的可疑事件。如果您的反詐欺系統質疑、阻攔或拒絕了過多良好交易，會讓您的優質客戶產生挫敗感。借助 FraudNet，您可以輕鬆辨識詐欺者和客戶，從而在保護線上管道的同時無需干擾客戶體驗。

FraudNet 帶來的收益

降低詐欺損失
詐欺捕獲率對確定您的反詐欺解決方案提供商的實效性十分關鍵，該數據每年都會出現在不同行業的報告中。FraudNet 提供了全面的解決方案，其詐欺捕獲率超過業界平均水平。

保護客戶體驗
FraudNet 提供的隱蔽且流暢的解決方案可以降低揀選率和詐欺誤報率，從而改善優質客戶的體驗，令您的業務獲得增長。

挫敗詐欺者
FraudNet 解決方案迫使被阻攔的詐欺者轉向更容易下手的目標，從而不斷降低我們客戶的長期受攻擊率。

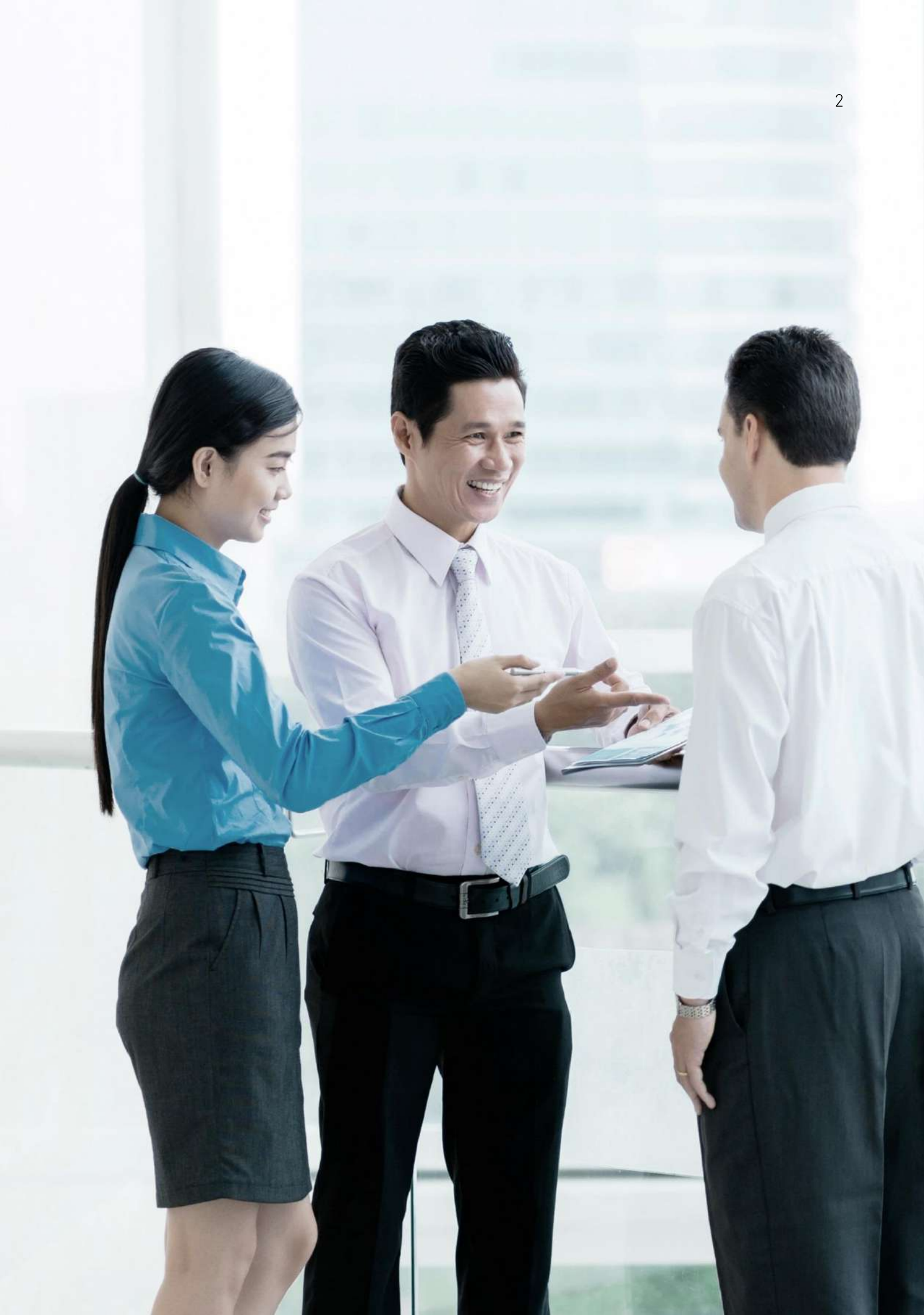
提高運營效率
FraudNet 解決方案可以提高效率，有助於減少浪費，改善風險管理。

FraudNet 組件

設備智慧
DeviceInsight。此項即時技術不需要標籤，不基於 cookie，讓企業在與詐欺者的競爭中領先一步，同時又不會干擾客戶體驗。設備資訊和收集器透過內部控制，保證每個事件有一個 DeviceInsight ID，無需外部調用、彈窗，也不用單獨與反詐欺解決方案提供商建立關係。

設備收集器十分隱蔽且注重保護隱私。收集器會從每個頁面收集百餘個不同屬性，將其與 HTTP 標頭資訊組合，然後產生 40 個字節的雜湊。除了 DeviceInsight，我們的專利——關聯時間差連結（TDL）值，還能帶來更高的檢測精度，深入洞察被使用的設備。

移動 SDK。移動設備和移動應用對數位事件是匿名的。移動 SDK 的構建目的就是用於本機原生應用，為設備辨識提供更高的檢測顆粒度。益博睿的研究人員已測試了數百種不同設備，不斷改進收集器針對 iOS 和 Android 設備的性能。除了測試諸多設備外，我們的團隊還會定期進行更新，以緊跟軟體更新換代的步伐，通常會領先於軟體發佈。



風險決策

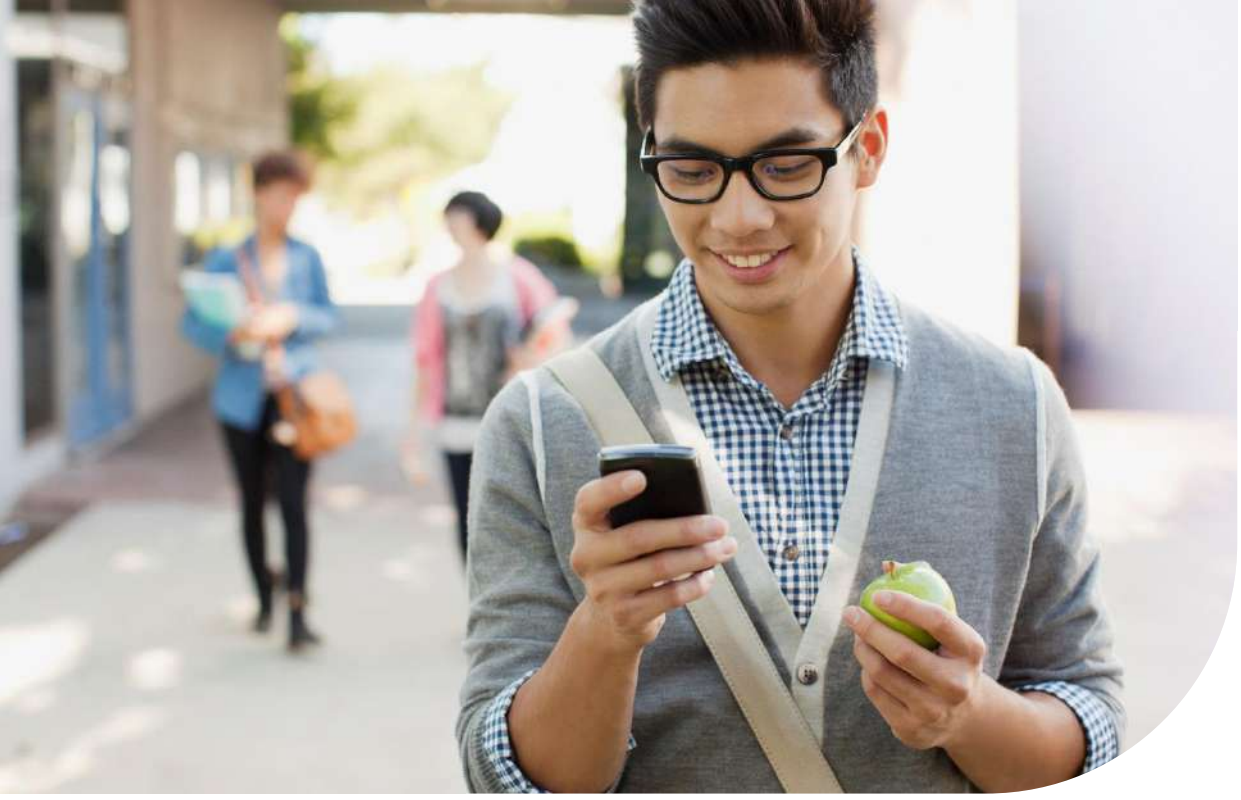
風險引擎。FraudNet 的即時風險引擎是一種高度可配置的策略驅動型風險模型，配備超過 600 條開箱即用式規則。除了每個客戶都可用的標準規則，還可創建自定義規則以針對特定行業內的特定詐欺模式。上下文數據、行為數據和設備數據的組合令 FraudNet 可以在更少詐欺誤報的情況下，辨識更多詐欺。

模型管理。FraudNet 幫助管理者靈活控制用戶界面內的所有模型，從而消除了對技術支援的依賴。管理者可以隨時添加、刪除或修改規則、規則得分或規則動作。所有對模型的更改都會即刻生效。

風險策略。風險策略必須與技術協同才能真正有效。這也是 FraudNet 的風險管理團隊與您自己的風險團隊直接合作來製定詐欺防範策略、積極強化風險模型，並共享跨層級詐欺資訊的原因所在。這一高度客製化的方式可將我們的經驗和您的需求進行最佳契合，以產生最為有效的詐欺防範策略。

周轉速度。FraudNet 的管理員可以創建自定義閾值的大小，以辨識那些重複使用數據或在同一設備訪問多個帳戶的詐欺者。該資訊可用於檢測網路機器人（BOT）活動、信用卡測試、破解帳戶和濫用免費試用等形式的詐欺。

惡意軟體。FraudNet 會檢測是否存在惡意軟體，儘管惡意軟體並不必定意味著該事件一定是詐欺，但確實表明用戶的認證資訊被盜用，因此該帳戶在將來的使用過程中需要加以特別防範。



用戶界面

案例管理。FraudNet 工作台以一種直觀、可配置的圖形用戶界面為調查人員提供所需的所有資訊。調查人員可從選出的事件隊列中搜索特定事件或行為，進行標記，採取不同行動，或按需求進行進一步搜索。將一次事件確認為詐欺，便可自動將此類預定義數據點添加到負面清單，以便在將來自動捕獲此類詐欺。在事件頁面內，調查人員可利用不同數據擴充和關聯，豐富事件資訊。

DataSpider。調查人員在搜尋與已知不良事件相關的詐欺時，可能會受到後期採證分析的困擾。有了 DataSpider，您不必再對此進行手工作業，而可透過姓名、電郵、電話、地址、用戶 ID 和加密信用卡卡號，在基於用戶的時間框架內，自動對相關事件進行遞歸搜索。一旦搜索運行，系統就會給出用不同顏色標記的結果，以顯示不同事件中的不同關聯。即使在詐欺者故意顛倒資訊以避開現有邏輯時，DataSpider 也能鎖定複雜的詐欺模式。

SketchMatch。DataSpider 根據用戶輸入數據進行事件關聯，而 SketchMatch 則透過設備數據達到同樣的目的。設備數據很難繞開或改變，並且詐欺者通常意識不到對此類資訊的收集。透過關聯分析，調查人員可以基於設備屬性查找關聯事件，從而發現潛在的可疑詐欺。

可配置清單。儘管 FraudNet 會向黑白名單的關鍵數據點引入正面及負面清單（包括電郵地址、DeviceInsight ID、地址和其他資訊），但不同行業有不同的需求和風險模式，適用於一個的未必適用於另一個。因此，我們創建了多個行業的專用清單，以提供多一重的防護。

分析

標準報告。6 種標準的開箱即用式報告可提供衡量 FraudNet 及相關風險團隊的效率所需的所有基本指標。每份報告都聚焦於風險組織內詐欺管理的不同方面。

基於支付方式的詐欺反饋報告和基於原因代碼的詐欺反饋報告。這兩種報告針對的是拒付率（Chargeback Rate），是電子商務及旅行商使用得最為廣泛的詐欺指標。透過被提交的拒付反饋或由分析師提交的詐欺事件反饋來衡量損失。

系統層摘要。該報告會給出整個企業組織總體績效情況的概覽，包含總銷售量和損失額。

揀選摘要。該報告會給出當前揀選隊列的概覽。

調查人員生產力。該報告衡量調查人員的績效，包括審核了多少事件，以及採取了什麼行動。此外還有附加指標，包括調查人員核准的審核中有多少是後續被認定為詐欺的。

規則層命中率。該報告幫助管理員基於獨立模型來衡量其系統中每條規則的效力。可給出各條規則代碼，規則代碼的當前設置以及一系列指標。其中關鍵指標之一是提升量，也就是規則效力的量化數字。

自定義報告。除了可用的標準報告，FraudNet 也可創建自定義報告。這些報告可隨時運作，或定期重複運作，也能保存或導出以供審核。用戶界面中可查看到的每個字段，幾乎也都可用於報告。

增強分析響應。這一擴展分析功能是對事件數據、設備數據、擴充數據以及高級風險數據的彙編，可用於機器對機器處理。該報告功能可將線上和線下業務數據整合入現有的數據倉庫，以供內部商業智慧工具進行分析。這些資訊的組合可用於辨識更多元的趨勢，並給出所有客戶的 360 度畫像。

數據擴充

第三方數據擴充。FraudNet 使用第三方數據擴充為調查人員提供更多背景資訊，以創建更為清晰的畫像。獲得諸如 IP 地址和 BIN 碼之類的資訊是不錯的方案，但是僅僅瞭解這些獨立要素並不會帶來更明智的決策。瞭解某個 BIN 代表國外帳戶，或是某個 IP 與帳單寄送地址位於同一城市，才能為您提供更多的背景資訊，幫助調查人員破解謎團。

行為背景。詐欺者都是投機分子，會在短期內嘗試進行盡可能多的詐欺，且通常在嘗試中展現出相同的習慣和模式，以期盡快走完流程而避免被檢測到。風險分析師透過不斷努力，致力於辨識出新詐欺趨勢和可疑詐欺特徵，並製定新規則，以便在捕獲詐欺者的同時保持較低的詐欺誤報率和揀選率。

有效的詐欺防範不僅是制止詐欺

您為詐欺防範所做的努力都是為了制止詐欺和減少損失。但是，一套行之有效的方案也會讓您的優質客戶更易於與您進行業務往來。如何才能兩者兼顧？首先就是避免所謂「萬金油」的一體適用型方式。相反，您應該針對每次交易運用適當的保護級別。

我們的反詐欺團隊在全球範圍內有近 300 名專家級人員，正致力於此而與企業展開協作。讓我們倍感自豪的是，過去一年間，我們幫助客戶篩查出了超過 150 億起詐欺事件，也就是每秒超過 3,300 件。多數客戶在進行日常操作（諸如線上購物或從移動端設備查看銀行存款）時，並不知道我們在幕後為他們的安全保駕護航。我們稱其為無擾保護，這也是理應實行的模式。我們的解決方案構建在數據、技術和分析之上，旨在制止詐欺分子而不干擾優質客戶。現如今，詐欺防範有助於促進業務增長，並打造流暢的客戶體驗。

益博睿台灣

台灣台北市中正區衡陽路 51 號
基泰國際商務特區（TIDC）11 樓 212 室
T: +886 2 2383 2268

探索益博睿
www.experianplc.com
益博睿決策分析、反詐欺和身份辨識業務
www.experian.com.tw

領英
Experian Asia Pacific

© 2020 益博睿香港有限公司台灣分公司 版權所有。

本文所使用的益博睿和益博睿標誌是益博睿公司的商標或註冊商標。本文提及的其它產品和公司名稱屬於其各自所有者。