PRESENTED BY estar

Credit to you

eStar's chief technology officer **Matt Neale** explains why online fraud is more than just stolen credit cards.

MOST OF US think of online fraud to be all about stolen credit cards ordering thousands of dollars of goods for delivery to far away countries. The reality is that online fraud is much closer to home and can be any purchase value with any purchase method, for any purchased product.

Online fraud is carried out by people (not credit cards!) and much of it originates from legitimate but dishonest buyers. Reducing online fraud means retailers need to do more than use a reputable payment gateway and just follow normal security practices.

The global average rate of online fraudulent transactions is 1%. With Australasia's annual online purchases nearing $20B, fraud risk is a significant issue, and equates to $200m a year to retailers purely in financial costs of lost payments or lost deliveries. When you factor in the unseen costs of reviewing, processing and servicing these orders, the true cost is 3x that. Add to that the intangible costs and risks to retailers in brand damage and perceptions from both customers and media, and the true scale of the impact becomes clear. This is what we know:

- 72% of all payment fraud appears online.
- 1% of all online purchases are fraudulent.
- $200m is the cost of online fraud to Australasian retailers.

Many retailers rely on a simple blacklisting of credit cards which have been proven fraudulent, or manual review of orders, but these methods don't scale well, and fail to detect dishonest behaviour by customers using their own cards. So called 'friendly fraud' scenarios are responsible for over 60% of all claims. For example, when a customer claims a refund from their credit card company by disputing they received the goods, claim they never ordered them, or that there was a problem with the product.

In a recent United States study, the two most adopted screening tools, Card Verification Number (CVN) and Address Verification Service (AVS), were rated among the six most effective. Screening an order against a customer's order history is the most adopted screening tool that relies on the Retailers own data, and is also rated among the top six for effectiveness. Geolocation by both IP and device position information is becoming more popular, and can reveal, for example, that an order is being placed from an address that is actually an empty lot, raising a red flag. Other emerging tools, such as device fingerprinting and website behavior analysis, are also attracting a lot of interest from Retailers.

The same study, highlighted 81% of retailers perform manual reviews after evaluation by an automated screen process, orders with more ambiguous transaction characteristics will be sent for deeper investigation by a loss prevention team. These experts will use additional data verification sources and apply their own judgment—developed through experience—to make a decision.

The proportion of North American retailers performing manual reviews of eCommerce orders, and the percentage of orders subject to review, have remained stable over the past five years, despite growth in eCommerce volumes.

Larger retailers review a lower percentage of orders than smaller retailers do. This may be because they have deployed more effective automated screening tools, so fewer orders get passed to manual review teams.

However, despite the largest retailers' low review rate of less than 10%, the sheer volume of orders they handle still means they face the need to employ sizeable review teams to do the work quickly and efficiently. The need to review and the time spent on this becomes a trade off to avoid introducing unacceptable delays into the order acceptance and fulfilment process.

Retailers should use tools that accurately profile purchasing behaviours. This means it will apply heuristic and algorithmic analysis to instantly compare orders against at least common risk metrics:

- Known fraudulent addresses.
- Data consistency analysis.
- Order velocity and value, and customer behaviour.
- Payment data validation and comparison.
- Address validation.
- Related orders and fuzzy pattern matching.

Market leading tools reduce online fraud to between 0.05% - 0.2% - depending on industry and region, against the global average of 1%.

Solutions need to be configurable to suit industry, regions and individual merchant risk profiles. Tools that incorporate behaviour analysis, and that have the reach to inspect and use aggregate knowledge and eCommerce data from multiple retailers and industries provide a notable advantage over those that rely in basic, common factors.

Regardless of the chosen eCommerce platform, a fraud prevention tool is a must, and retailers in all industries can reap the benefits.

As global markets become more accessible, and retailers use the online channel to grow at unprecedented rates (compared to traditional retail) into these markets, the benefits of accurate and reliable automation allow for more effective deployment of loss prevention teams, providing increasing sales growth, without having to invest heavily in head count, whilst maintaining (or improving) service levels and reducing fraud. ■

PRESENTED BY estar