BIZCOMMUNITY

Beating online fraud

According to Peter Harvey, the founder and CEO of payment gateway provider PayGate, Yuppiechef is one of the most successful online businesses staying one-step ahead of fraud attempts.

"We tell our clients that good business processes are the final line of defence against online fraud and this is a great example. It has put a lot of thought and effort into developing systems to beat credit card fraud."

It did not start out that way, acknowledges Yuppiechef MD, Andrew Smith. "When we started out in 2006, we were so small that when the first order came in we high-fived and did a happy dance. The idea that we might be targets of fraud did not even enter our heads. The first time it happened, we got a chargeback on an expensive mixer we had delivered to an address in Johannesburg.

"When we looked back at the original order, there were some clear danger flags, so when the same person tried the same thing again we actually worked with the courier company and the police to set up a sting. When the suspect appeared before the magistrate, he just said he had been collecting the package for a friend - there was insufficient evidence to convict him and he walked away. That's when we realised that we were on our own when it came to combating fraud - we're just too small to be worth serious police attention."

Developing systems

Smith and his team set out to develop systems that would stop fraud attempts in their tracks. "We have an automated process that picks up potentially suspicious transactions and flags them for human attention. We look at what the order is and where it's going - we can tell a lot from names, addresses and email addresses and even from typing style and language use. Once you know what the signs are, it's actually fairly easy to spot."

If his team has reason to suspect the transaction is a fraud attempt, we check their Facebook page, or ask for some additional ID or a landline telephone number. People who are legitimate buyers will provide that with no problem, it's only the fraudsters who have a problem."

It is important to be as non-invasive as possible. "We don't want to annoy 99.9% of our real customers with extra processes just to catch the 0.1% who are fake - that's why we don't ask for an ID number on checkout."

Fortunately, says Smith, the company is not a particularly attractive target for fraudsters. "Our goods are not that easy to resell - they have nothing like the street value of a computer. However, we do sell vouchers and cookware, which are where we tend to get problems. Moreover, the problem is small enough that if we are burned, we can adjust our systems the next day and not suffer a significant loss. Only about one out of 100 orders we get is a fraud attempt - we'd have a bigger problem with shoplifting if we were a physical store."

Backup systems

The company backs up its own fraud checks by using PayGate's PayProtecter, which provides an extra layer of automated checks for suspicious transactions. "We don't want to rely only on the system because those reports come the next day and 85% of our orders leave the same day they are placed. But it's a very useful check."

It does not use the 3D Secure online PIN system from MasterCard and VISA because "it's a hassle for our customers and we'd lose sales. But if fraud was a bigger issue for us we'd certainly use it."

PayGate's Harvey says this client exemplifies the multi-tiered fraud protection strategy it recommends for all its clients. "There's no magic bullet, no one thing you do can eliminate the risk of fraud. Nevertheless, any business can dramatically reduce its risk of fraud by using a combination of its own systems, our system and 3D Secure. Not implementing anything at all is asking for trouble."