BIZCOMMUNITY

What you need to know about mobile retail fraud

By Leigh Andrews 16 Feb 2015

You know the field of digital security is booming when there's a need for the day job titled 'retail industry fraud expert'. These are people like Aaron Press, director of e-commerce and payments at LexisNexis Risk Solutions.

The fact that mobile or m-commerce channel adoption is skyrocketing as merchants take advantage of the availability of mobile devices should be a good thing. Sadly, when you realise that the cost of m-commerce fraud is now actually outpac its growth, the picture tint fades from rosy to gloomy grey.

That's why a new study by LexisNexis has been released, just as Apple Pay and other mobile payment solutions achieve wider penetration. I pressed Press for details on what we're really facing...

What's the day job of a retail industry fraud expert like?

Press: It can be like drinking from the proverbial fire hose. E-commerce continues to grow at incredible rates, but it remai vulnerable to fraud due to the remote nature of the channel. Fraudsters understand this, and constantly adapt their strategi to defeat new strategies to stop them. That means fraud teams and tools must also constantly adapt.

What prompted the new study on m-commerce fraud?

Aaron Press

Press: We have been conducting the 'true cost of fraud' study for several years, focusing on traditional e-commerce. Mo recently, m-commerce has been gaining attention, and its growth has been accelerating as smartphones and tablets overt the market. We realised that e-commerce merchants weren't typically making a distinction between traditional and mobile transactions, primarily because they aren't that different from a payment processing perspective. As fraud experts, howev we believed that any new channel carries new potential risks, and wanted to better understand how that might be affecting the market. By adding mobile-specific questions to the survey, we were able to clearly see the differences between channels. Last year, we decided that the findings were worth a separate analysis effort. This year's report is the second m commerce study.

What's the key reason that m-commerce is attracting fraud at a disproportionate rat over online fraud?

Press: New channels have always meant new levels of complexity, which require a different set of processes. It's very difficult to anticipate all the potential challenges. Fraudsters have always been quick to identify and exploit vulnerabilities in new systems. Mobile is no different. The good guys have to find and close the gaps.

Talk us through the losses m-commerce companies experience when dealing with fraud.

Press: M-commerce losses are similar to those experienced in other channels, but as the 'true cost of fraud' study highlights, the costs are often higher than merchants realise. In addition to the value of the lost merchandise, merchants d with payment processing and charge-back fees, the costs of investigating the fraud, logistics fees, the cost of replacemen merchandise, and other assorted administrative overhead costs. In m-commerce, that adds up to $3.34 in total costs for every $1.00 of fraud.

That's shocking. Who's most at risk, and why?

Press: Now that we have a better understanding of the risks associated with mobile commerce, we can create processes, rules, and models that help to identity problematic transactions before they are completed. Those most at risk are organisations that fail to differentiate between mobile and traditional e-commerce from a payments and fraud perspective a integrate that knowledge into their fraud prevention practices. This is important even if a company has not made a conscic effort to enter the mobile channel; the nature of today's mobile devices means that e-commerce merchants have mobile customers, whether they know it or not.

Let's be proactive. What can we do - as retailers and consumers alike - to better protect ourselves?

© Seewhatmitchsee – 123RF.com

Press: For retailers, the key is to collect as much information about the transaction as possible, and to use that data in a risk-based, layered approach. By examining a variety of incoming signals, such as cart contents, IP address, device attributes, and identity information, merchants can develop processes that both stop fraud and enable sales. Consumers should focus on common sense measures to protect their identities. They should transmit financial information only over secure networks, ensure they are shopping with reputable merchants, and keep an eye on payment accounts to identity fraudulent transactions as soon as possible.

Click here for more on the six trends for 2015 that'll change the face of mobile transactions, as discussed at the recent Payl event, and click here to view the LexisNexis 'true cost of fraud' mobile study PDF.

ABOUT LEIGH ANDREWS

Leigh Andrews AKA the #MilkshakeQueen, is former Editor-in-Chief: Marketing & Media at Bizcommunity.com, with a passion for issues of inclusion, belonging, and of course, gourmet foo drinks! Now follow her travel adventures on YouTube @MidlifeMeander.
View my profile and articles...