internet RETAILER® portal to e-commerce intelligence

August 31, 2015, 7:30 AM

Card-not-present payment fraud is poised to grow

BY ALLISON ENRIGHT Editor

Already accounting for 25% of losses due to fraud globally, card-not-present fraud is expected to grow as U.S. card issuers roll out tougher-to-counterfeit chip cards.

etailers may soon be tussling more with criminals who try to fraudulently use payment cards to pay for online orders. because U.S. banks are issuing replacement credit cards to consumers that contain a microchip designed to make harder to counterfeit and use in stores. But those chips cards won't deter online fraud, because computers lack chip eaders. That's leading payment industry insiders to predict criminals will attempt more fraud on the web.

arch from The Nilson Report, a payments industry publication, says U.S. credit and debit card issuers, acquirers and ants already bore the brunt of nearly half (48.2%) of the $16.31 billion in losses due to all forms of payment fraud globally last year, despite accounting for only 21.4% of global purchase volume on payment cards. That's because much of the rest of the world has already phased in chip cards, following what's called the EMV (short for EuroPay, MasterCard, Visa) card standard. The United States is the last large nation to make the shift to EMV.

Use of counterfeit cards cost U.S. issuers, acquirers and merchants $3.9 billion last year, accounting for 23.9% of total global fraud losses. With the Oct. 1 deadline for chip cards in the United States around the corner, Nilson Report expects some of that fraud activity to move online. After Oct. 1, any U.S. merchant that has not deployed chip card readers in its stores will assume the burden for any fraud that occurs on credit and debit card purchases in its bricks-and-mortar locations. Until now, in a face-to-face, or card-present, transaction, the card-issuing bank assumes liability once it approves the transaction.

The United States has the further dubious honor of being the world leader in card-not-present fraud, in which a criminal uses payment card information that is not their own to pay for something online, through a call center, on a mobile device or by mail order. The Nilson Report estimates 25% of total global fraud losses last year—roughly $4.08 billion—was due to card-not-present fraud losses. It did not break out a dollar estimate by country, but says the United States leads in card-not-present losses.

Over the next five years, "[card-not-present fraud] will continue to grow as EMV becomes ubiquitous worldwide, leaving online sellers the primary focus of experienced, sophisticated criminals," writes Nilson Report publisher David Robertson, in a report released this month that analyzes 2014 fraud costs.

The Nilson Report says the United States is a hotbed of card-not-present fraud because it is a leader in card-not-present sales. Many online retailers in the United States don't use recommended security protocols, such as 3D Secure authentication, that may limit fraud out of concern the extra steps may make consumers abandon their purchases. 3D Secure authentication is branded as Verified by Visa or MasterCard SecureCode and requires a consumer to enter a password for that service to complete the checkout process. If a consumer hasn't set up an account with the corresponding service, they must do so before they can complete the order.

"Online merchants in the United States have deployed sophisticated predictive analytics to keep fraud in check but have not embraced 3D Secure as a further defense," Robertson says. "U.S. merchants worry less about merchandise lost to fraudsters and more about losing good sales to shopping cart abandonment from what they see as the tedious 3D Secure process."

Card-not-present fraud also rose in the Asia-Pacific region due to the growth of e-commerce sales there. Asia-Pacific web sales grew 37% from 2013 to 2014, according to Internet Retailer estimates, the highest growth rate of any region.

Click here to read an Internet Retailer magazine story on how retailers can prepare for the EMV liability shift.

TOPICS: 3D Secure authentication, card-not-present fraud, chip cards, e-commerce sales, EMV, online orders, recommended security protocols, The Nilson Report, U.S. credit and debit card issuers

---

Be the first to comment.