Vesta Report: Card-Not-Present Fraud is Becoming Increasingly Sophisticated, Creating New Threats for Merchants Across the Globe

Global fraud analysis shows CNP fraud costing merchants millions in annual revenue with fraudsters getting more sophisticated with their attacks every quarter

PORTLAND, Ore. – September 22, 2021 – Vesta, an end-to-end transaction guarantee platform for online purchases, today released its first Global Card-Not-Present (CNP) Fraud Report, which includes an analysis of millions of digital transactions from the first quarter of 2020 through the first quarter of 2021 to track how CNP fraud evolved during that time frame. The overall percentage of global transactions its system identified as being potentially fraudulent ranged from 10 to 13%, with the average value of each fraudulent transaction ranging from $126 to $155. Fraud attempts, however, are not evenly distributed: fraudulent attempts at individual merchants ranged from 0.8% to over 30% depending on business vertical and geography.

A CNP transaction occurs when a sale is made without the customer physically presenting their credit card to the merchant, and when a CNP transaction turns out to be fraudulent, the liability lies with the merchant. When a merchant approves a fraudulent CNP transaction it leads to a chargeback, and chargebacks come with fees - sometimes as high as $25 per incident. In the first quarter of 2020 Vesta found that 13% of overall transactions were likely fraudulent, and therefore it blocked those transactions to protect its customers. It is important to remember that 13% is an aggregate number, inclusive of both high and low-risk merchants. For low-risk merchants, Vesta approved as many as 99% of all transactions, but for high-risk merchants that approval rate varied greatly depending on fraudulent activity. For high-risk merchants that don’t have a solution like Vesta’s in place, approving so many fraudulent transactions can have a dire impact on both revenue and overall brand reputation.

“If you’re an eCommerce business doing 5 million transactions per year and 13% of those are fraudulent, you’re looking at 650,000 bad transactions, and if each one of those comes with a $25 chargeback fee, you’re now looking at more than $16 million dollars in fees,” said Ron Hynes, CEO of Vesta. “On the other hand, if you decline too many legitimate transactions in an effort to fight fraud, you end up with significant losses. For example, if that same merchant doing 5 million transactions per year has an average order value of $125 and blocked 30% of all transactions when only 13% were fraudulent, they’re now losing more than $100 million in annual revenue. That’s what makes CNP fraud such a challenging problem to deal with - you have to strike the perfect balance between fighting fraud while maximizing approvals of legitimate transactions."

There are five operating systems that make up the majority of eCommerce orders - Android, iOS, Linux, OS X, and Windows. To gain a better understanding of how operating systems impact CNP fraud, Vesta analyzed the percentage of fraudulent transactions made on each as well as the average value of those transactions. It found that Android is the operating system with the highest percentage of fraudulent transactions - as high as 26% in the first quarter of 2020 - but the lowest average dollar amount, suggesting fraudsters use it frequently for lower value transactions. The value of fraudulent transactions is highest on OS X and Windows, indicating fraudsters make their most expensive attacks via desktop.

Another critical element of Vesta's report is an analysis of CNP fraud with direct linkage compared to indirect linkage. Direct linkage means there's some common connection within the transactions that merchants can look for as signs of potential fraud - for example, if five orders come in at the same time, for the same item, and from the same email address, that's a clear sign the transactions could be fraudulent. Indirect linkage means transactions are linked through a more complex web of elements, often a sign of more sophisticated fraudsters attempting to cover their tracks, which makes it very difficult for merchants to spot.

"Unfortunately, we're seeing fraudulent transactions with indirect linkage increasing across the board, and the average value of those transactions is higher than those with direct linkage, making it an even more expensive and complicated problem for merchants to navigate," said Hynes. "The only way to effectively identify and prevent CNP fraud with indirect linkage is with machine learning, and it's critical to use models that have been trained against millions of global transactions and can therefore draw connections that humans simply can't see."

You can view Vesta's full Global CNP Fraud Report here. For more information on Vesta and its transaction guarantee and fraud prevention solutions please visit www.vesta.io.

About Vesta

Vesta is the only instant, end-to-end transaction guarantee platform for online purchases, delivering unparalleled approval rates, a better customer experience and eliminating fraud for leading brands in telco, e-commerce, travel, and financial services. Using machine learning backed by 25 years of transactional data history, Vesta increases approvals of legitimate sales for its customers, while eliminating chargebacks and other forms of digital fraud, driving the true cost of fraud to zero and transferring 100% of the liability for fraud, including chargeback processing, so customers can focus on increasing sales. The company is headquartered in Portland, OR, with offices in Atlanta, Miami, Ireland, Mexico, and Singapore. For more information visit www.vesta.io.

Press Contact for Vesta
Michelle O’Rourke
Clarity PR for Vesta
vesta@clarity.pr