BRING ON CYBER MONDAY:
E-COMMERCE MERCHANTS AND FRAUD

October 2014

According to the National Retail Federation, 44% of consumers plan to do their holiday shopping online this year, and will spend an average of $804. For consumers, it is a prime time of year for unbeatable deals and coupons. For cybercriminals, it is an opportunity to commit e-commerce fraud as they hope to get lost in the noise of the incredibly high transaction volume that is a result of holiday shopping season.

What merchants can anticipate the highest volume of fraud, and what is the average value of a fraudulent transaction by merchant? RSA has gathered insight from the billions of e-commerce transactions we secure each year, and here are some of the trends we are seeing based on dated from Q3, 2014.

TOP MERCHANT CATEGORIES FOR E-COMMERCE TRANSACTIONS

Following are the top ten merchant categories for e-commerce transactions:

- Airlines (44%)
- General Retail (17%)
- Computers/Electronics (12%)
- Telecom (mobile phones, apps, etc) (6%)
- Money transfer (5%)
- Automotive (3%)
- Toys (3%)
- Clothing and shoes (3%)
- Restaurants and dining (2%)
- Education (2%)

1 Consumer Perceptions on Privacy and Security, Ponemon Institute, October 2014
AVERAGE VALUE OF FRAUD TRANSACTIONS

While there are several indicators of fraud, one of the most common is the average value of a transaction. The chart below shows the average value of legitimate transactions vs. fraudulent transactions, with the fraudulent transactions most always bearing a significantly higher value than an average legitimate transaction. For example, an average ticket purchase online is $225 while an average fraudulent purchase in the same category is $1,050, more than four times that value.

![Average Value of Fraud Chart](image)

TOP MERCHANT CATEGORIES AFFECTED BY FRAUD

As consumers, we like to indulge once in a while with a random getaway, new electronic gadget, or the latest fashion trend as seen by the average value of e-commerce transactions. But cybercriminals find it even more enjoyable to use stolen payment cards to indulge themselves with vacations, cash, and computers – and even to pay their monthly household bills. The following chart represents the top merchants affected by fraud transactions.

![Top Merchant Categories Chart](image)
CONCLUSION

According to a recent study, one out of every two consumers stated their personal or financial data was compromised in a data breach. Despite, 45% of the same respondents stated it has no effect on their use of credit or debit cards. Financial institutions and retailers must be prepared to make the investments in technology to manage fraud risk in e-commerce.
Phishing Attacks per Month

RSA identified 24,794 phishing attacks in September, marking a 25% decrease from August. Based on this figure, RSA estimates phishing cost global organizations $240 million in losses.

US Bank Types Attacked

U.S. nationwide banks saw a decrease in phishing volume in September – from 71% to 60%. Phishing against credit unions remained the same while regional banks saw an increase from 18% to 27%.

Top Countries by Attack Volume

The U.S., the UK, China, the Netherlands, and Canada were the top five countries targeted in September with 80% of total attack volume.
Top Merchant Categories Affected by Fraud
In the third quarter of 2014, the merchant category most affected by e-commerce fraud, with 46% of fraudulent transactions, was airlines and travel. The second most affected merchant category, with 16% of fraudulent transactions, was money payment processors.

Top Countries by Attacked Brands
Brands in the U.S., UK, India, and Canada were targeted by half of all phishing volume in September.

Top Hosting Countries
Hong Kong remained the second top hosting country for phishing for the third straight month with 12% of total attacks while the percentage of attacks hosted in Germany nearly doubled, from 4% to 7%.