Crazy Things You Wouldn't See in a Restaurant
"Criminals in the customer payment process"

We have all turned to digital commerce as a lifeline during the lockdown. As crazy as the pandemic has been, it is good to make light of crazier things that should not happen. The Media Trust and RH-ISAC are exploring some of those things in this series, *Crazy Things That Happen in your Online Store Every Day*.

Crazy Things #2 – Payment Fraud

Point of sale devices operated by criminals and broadcast customer data.

Due to the Covid-19 pandemic, we have all been home and the opportunities to dine out have been limited. Imagine that a customer has gone out to an appropriately socially distanced dinner venue and has a wonderful experience. Also imagine the customer's surprise, when at the end of the meal as they go to pay the check, not only their server and other trusted employees are operating the point of sale device, but a whole host of other people that don't work for the restaurant are taking notes and even taking pictures of the credit card during the payment process. Crazy, right?

Would you hand over your credit card to be processed in the presence of these people, including some of whom might be criminals? Would you return to a restaurant like this, one that doesn't have adequate payment security in place, or which allows third parties access to your payment information?

Seems crazy, right? But this happens on many eCommerce websites!

Our engagement with restaurant websites and mobile apps reveals there are a host of unregulated and unmonitored activities present in cart and checkout pages. Where one would expect to find a single payment processor, we have found a plethora of players, including masked and suspicious domains leading to the unauthorized exfiltration of data. This creates an enabling attack surface for credit card skimming and Magecart breaches to occur. Common payment fraud breaches include:

- **Magecart/Digital Skimming** - Magecart is a type of malware attack often delivered to a site by way of malicious third-party JavaScript code that steals consumers' personal information from a checkout page, including credit card numbers, email addresses and passwords. Magecart attacks are sophisticated and well disguised, often running undetected for weeks or months.
- **Customer Data Leakage** - Personally identifiable information ("PII") can be exfiltrated from your website by competitors or bad actors easily through third-party malicious code or gathering data from cookies that are not secure or transmit information through unencrypted channels.

Overcoming crazy isn't an insurmountable feat.

For 15 years we have been helping companies with deep 24x7, 365 monitoring of their websites to detect malware and inventory every third-party vendor on their ecosystem. We establish what each vendor is doing and evaluate all data collection activity on your website to assess unauthorized data exfiltration.

Find out best practices in monitoring and what is happening on your website.

FIND OUT!

THE MEDIA TRUST
We know digital security.