CASE STUDY

Restaurant Group Remediates BIN Attacks After Help From MSP Partner

PARTNER TYPE

Managed Service Provider

CUSTOMER COUNT

51-250

LOCATION

North Carolina

"Partnering with Coalition has helped us grow our customer base and reach businesses we might not have otherwise. As an MSP, we can bring our own security expertise into the existing relationship with the policyholder."

— Mike Ouimet,
President and Co-Owner,
Wincourse Technologies

A restaurant group with more than 30 franchise locations across the United States was struggling to figure out why an overwhelming majority of customers were experiencing credit card declines. The Virginia-based company exhausted all avenues of support, contacting its point-of-sale (POS) system and credit card processing providers, before spending thousands of dollars to replace all of the technology — but nothing remediated the issue.

Eventually, the company contacted Coalition and requested a referral to an IT service provider. We referred the restaurant group to Wincourse Technologies, one of our established managed service provider (MSP) partners. After the initial meeting, Wincourse suspected that the suspicious activity might be the result of attempted credit card fraud.

Wincourse determined that not having CAPTCHA enabled on the restaurant group's website was causing the declined credit card transactions and allowing banking identification number (BIN) attacks to occur. Wincourse helped the company enable CAPTCHA — which immediately stopped the BIN attacks — and recommended additional security improvements based on external scans conducted using Coalition Control®.

As a result of the referral, Wincourse helped the restaurant group successfully resolve a serious security issue. "Partnering with Coalition has helped us grow our customer base and reach businesses we might not have otherwise," said Mike Ouimet, President and Co-Owner, Wincourse Technologies. "As an MSP, we can bring our own security expertise into the existing relationship with the policyholder."

The quick engagement and actions of Wincourse not only assisted the company in a high-stress situation but also led to a scope of work (SOW) that resulted in approximately $4,500 in new revenue for investigating the source of the BIN attack and for providing remediation support.

The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law. Facts may have been changed to protect the privacy of the parties involved.