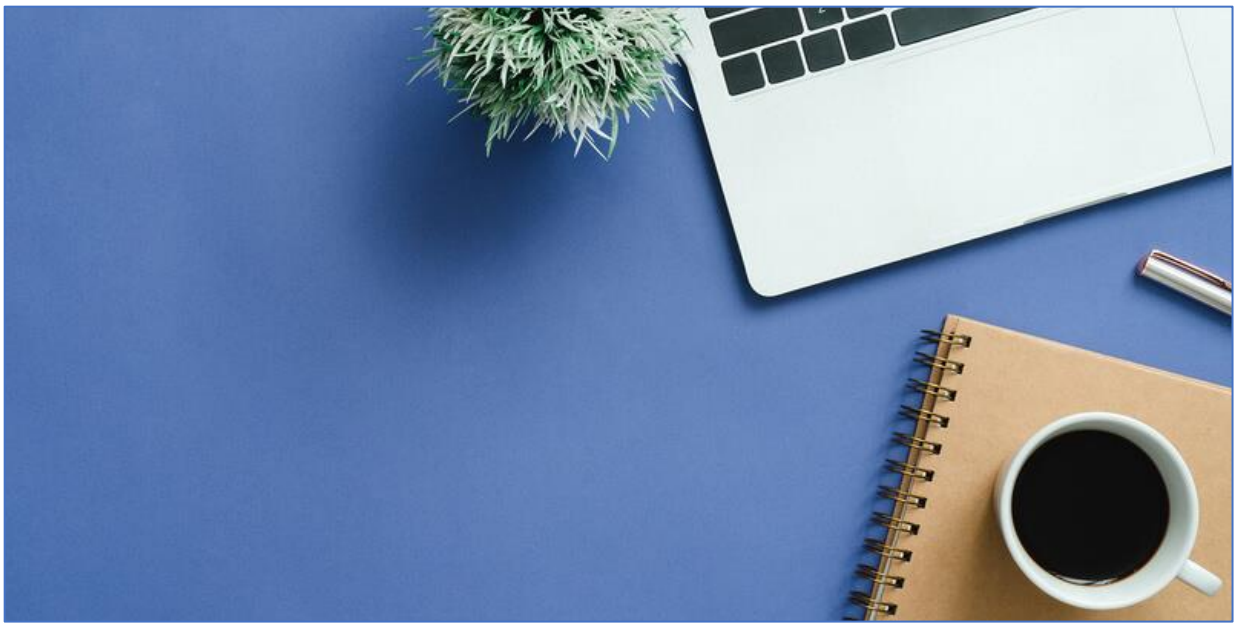
Victor Font
CONSULTING GROUP, LLC

Case Study

Coach's Oats vs. Coco Jimenez, et al

TABLE OF CONTENTS

Author: Victor M. Font Jr.



INTRODUCTION

Normally, when WordPress-WooCommerce solutions are deployed, they simply work and continue working for the life of their deployment. Yes, there is the occasional glitch when an end user makes a mistake or a plugin or maintenance update goes sideways, but this is the rare exception, not the rule. The rule is smooth sailing for all ships at sea.

Smooth sailing that is, until Coco Jimenez threw a monkey wrench into the works for Coach's Oats. Who is Coco Jimenez, what's Coach's Oats, and what do they have to do with each other? This case study explains. First, let's learn about Coach's Oats.

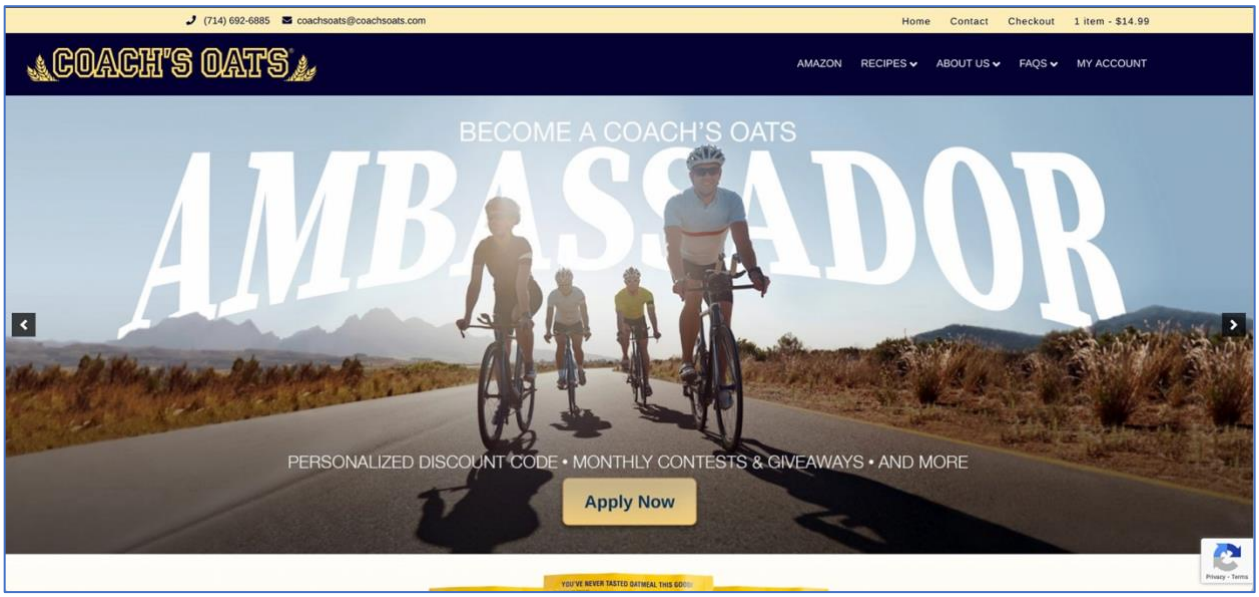


Figure 1: Coach's Oats website

Coach's Oats

Coach's Oats is one of Victor Font Consulting Group's oldest and dearest clients. We deployed their WordPress-WooCommerce solution way back when. It was so long ago, that none of us on either side of the equation can pinpoint how long we've been working together. They are one of our first and longest-term monthly care plan subscribers. We've grown a lot through this website, and since the pandemic we've had some challenges, but nothing like the havoc perpetrated by Coco Jimenez, et al.

Coach's Oats is a small business in Brea, California. They primarily package and sell delicious steel cut oatmeal. When able, they sometimes add organic and whole grain products to the online inventory. Among their revenue streams are a store on Amazon and the website we built and maintain. For a modest online presence targeting the United States and Canada, the website generates healthy sales. Their Ambassador Program offers purchase discounts and perks for their Brand Ambassadors, which is a smartly strategic and popular form of affiliate marketing.

When the pandemic spurred consumer hoarding, we had to limit quantities sold online. Their warehouse also emptied of product multiple times forcing us to suspend online sales until supplies were replenished. We don't backorder oatmeal in WooCommerce. Until Coco, this is the worst we've experienced in years.

Early in the history of this website, we had problems downloading negotiated UPS rates so Coach's Oats could provide the greatest shipping value to their customers. Greater quantities of oatmeal can be heavy to ship. Standard UPS rates are high for heavier transports. Coach's Oats successfully negotiated much lower rates than the standard for their UPS shipping, a benefit for all their customers.

The rate retrieval from the UPS Application Programming Interface (API) had been working since first setup. We never had problems with UPS rates after it went live. Now, the long-negotiated rates disappeared from the feed and only standard rates were coming back from UPS. We checked the website up and down and concluded the problem was likely with the UPS side of the feed.

The rate issues were traced to a programming change in the UPS API. The API was quietly modified without notifying its subscribers, the external developers that write interfaces to it for their clients. The change somehow affected the Coach's Oats negotiated rate feed. Only standard rates were being sent to the site through the API after the change.

UPS couldn't fix the problem either. Whatever happened trashed the old, negotiated rate feed and UPS couldn't restore it. The solution UPS suggested was to ask Coach's Oats to open a new UPS account so the negotiated rate feed could be attached to that account instead of the old one. UPS's solution ultimately worked after jumping through all their hoops. But these experiences, until Coco, are standard business issues with relatively easy resolutions for online stores. These are the type of online business issues that are common to the medium.

As things returned to normal, sometime in the April 2021 timeframe, the Coach's Oats team began experiencing an increase in their payables to Payeezy, the payment gateway that interfaces with their bank. The accumulating fees are for failed credit card transactions, and they were being flooded with them!

Payeezy charges $.25 per failed credit card transaction. It's a small amount to pay if a good customer enters their credit card details incorrectly. After all, we all do it at times. We transpose a number, forget the expiration date, or enter an incorrect CVV code.

As an online proprietor, if I only had to pay a few cents a couple times a month for my regular customers, then it's no big deal of an expense to absorb. But when you're suddenly flooded with fees and the transactional costs run into the thousands of dollars, and you don't know why? Panic sets in. It's not easy for a small business to cover that much loss so quickly. And it doesn't matter how big of a small business you are. Quick, large losses are cause enough to make the owners of any size business panic.

Coco Jimenez

#31291 Coco Jimenez	Jun 14, 2021	Failed	Coco Jimenez, 1265 Fern Lake Ave, Brea, CA 92821 via UPS	$11.89	31291
#31290 Coco Jimenez	Jun 14, 2021	Failed	Coco Jimenez, 1265 Fern Lake Ave, Brea, CA 92821 via UPS	$11.89	31290
#31289 Coco Jimenez	Jun 14, 2021	Failed	Coco Jimenez, 1265 Fern Lake Ave, Brea, CA 92821 via USPS Flat Rate Shipping	$5.20	31289
#31288 Coco Jimenez	Jun 14, 2021	Failed	Coco Jimenez, 1265 Fern Lake Ave, Brea, CA 92821 via USPS Flat Rate Shipping	$5.20	31288
#31287 Coco Jimenez	Jun 14, 2021	Failed	Coco Jimenez, 1265 Fern Lake Ave, Brea, CA 92821 via USPS Flat Rate Shipping	$5.20	31287
#31286 Coco Jimenez	Jun 14, 2021	Completed	Coco Jimenez, 1265 Fern Lake Ave, Brea, CA 92821 via USPS Flat Rate Shipping	$5.20	31286
#31285 Coco Jimenez	Jun 14, 2021	Completed	Coco Jimenez, 1265 Fern Lake Ave, Brea, CA 92821 via UPS	$11.89	31285
#31284 Coco Jimenez	Jun 14, 2021	Failed	Coco Jimenez, 1265 Fern Lake Ave, Brea, CA 92821 via USPS Flat Rate Shipping	$5.20	31284

Figure 2: Screen Print of Coco's earliest transactions

I stepped into the investigation and reviewed the above WooCommerce order summary screen. The list shows 6 failed orders and 2 completed.

The Coach's Oats team discovered the failed credit card transactions were originating from the website's WooCommerce orders. There were suddenly a multitude of failed orders. Nothing about most of them were alike, other than they were for the smallest possible purchase. The addresses were sometimes the same, but fake. The email addresses were mostly different and always fake, and the IP address would sometimes match across two or three order attempts, but that was only a small percentage. Most of the bad orders had different IP addresses.

The failed credit card attempts were being documented as quickly as one per minute apart or less. The system was getting pounded aggressively in relatively small but persistent timeframes. What's worse, not one security measure in place on the site sounded an alert. Whatever or whomever was doing this found an open door and they invited themselves in to do as much damage as they could while trying to find a credit card with room for their greedy gain.

With high-speed notifications like this streaming in, my first thoughts were, "Could this have been a bot that had penetrated the system, auto entered the orders, and caused us to receive these very fast gateway

notifications?" And "Could this be someone directly manipulating the gateway through some back door process?"

I dreaded both prospects because both scenarios are above my paygrade. I would have to bring in the big guns for this level of security testing. So, I tucked the idea away in the back of my brain that Payeezy might be the actual target of these attacks and started with the lowest hanging fruit, examining the orders.

The first order I investigated in depth was written by someone using the name Coco Jimenez. It could be an alias, so I'll refer to this individual and all the Cyberthieves involved in this Cybercrime collectively as Coco.

Coco was one of the earliest failed transactions in the queue. He/she/they also used this name for many other failed transactions. We don't know if this is a real or fake name, but in the last few failed orders in his queue, its spelling changed from Coco Jimenez to Coco Jimenes with an 's', which is assumed to be an apparent attempt to disguise his last name or circumvent a security measure I put into place. The name change occurred right after I blocked access to the site for anyone named "Coco Jimenez" with the 'z'.

Assuming the last name changed to evade the blocking software, I suspected this was probably a live person and not a bot. It would be an awfully smart bot to change a last name to evade blocks this fast, but it's possible. Some hackers are incredibly talented and crafty with their penetration bot programming. But again, bots are above my paygrade.

The one thing common with these orders is all the failed credit card transactions. Each order had literally accumulated hundreds, if not thousands of bad credit card verifications. Remember, these failed credit card transactions are costing Coach's Oats $.25 each. Dropping quarters at this rapid pace adds up to big dollars.

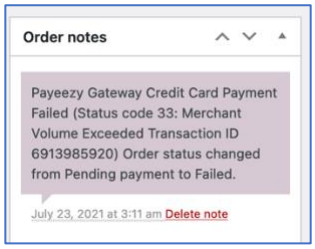


Figure 3: Payeezy Order Note

The cards were most often rejected because of no available credit as in the example to the right. "Merchant Volume Exceeded Transaction ID" is Payeezy speak meaning the card's credit limit was spent. Sometimes, the CVV code couldn't be verified. Once in a very great number of attempts, a card received authorization and the small fake order went through. These orders are marked as "completed" in Coco's transaction list.

The first time a credit card payment fails with the Payeezy gateway, it changes the WooCommerce order status to failed as documented in the screen capture of the order note above right, but that doesn't end the transaction. Payeezy displays a message to the user on the front end that says something went wrong and to try again. It displays the try again payment entry screen (next page) every time it records a failed transaction.

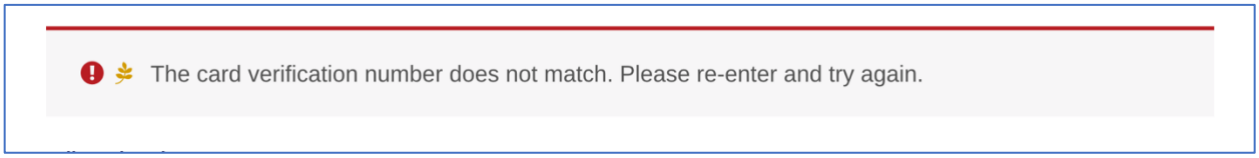


Figure 4: Payeezy error message

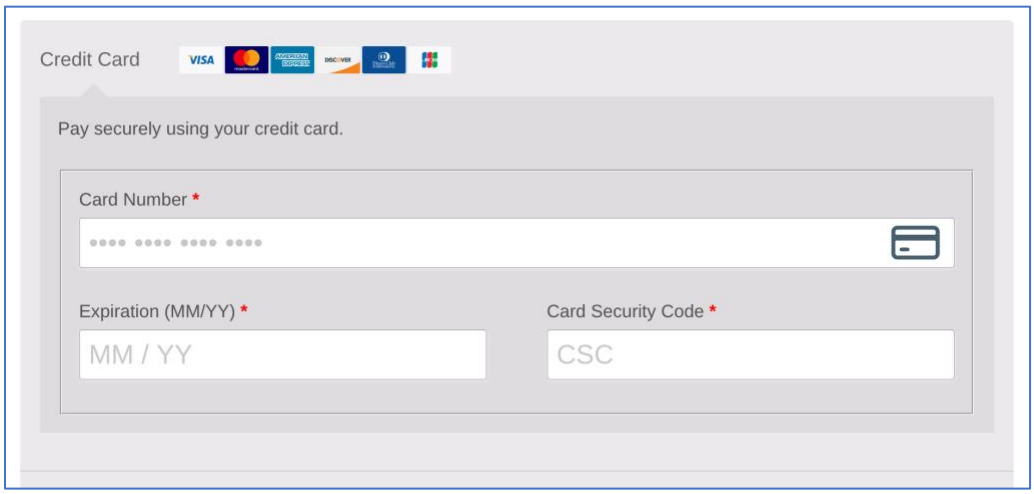


Figure 5: Payeezy Payment Entry Screen

We've learned this cycle can seemingly function as an endless loop. There's no way to limit the number of allowed failed transactions in WooCommerce with the Payeezy Gateway, which could in fact be a zero-day security vulnerability or a purposefully engineered software feature designed to raise revenue. A zero-day vulnerability is a software security flaw that is known to the software vendor, in this case Payeezy, but doesn't have a patch in place to fix the flaw. A purposefully engineered software feature to raise revenue through bad credit card transactions is corporate malfeasance. In either scenario, they are issues Payeezy needs to address.

Since WooCommerce doesn't store credit card numbers and we, as administrators, can't see customer payment details, the only record we have is the Payeezy order note which is returned from the Payeezy API. We can only assume that each failed credit card verification is for a different credit card number. How else can you explain the thousands of failed transactions with nothing in place to stop them? It's quite an exploit!

Working with a Payeezy representative, Coach's Oats was able to limit the number of daily failed transactions in their Payeezy account. They set the limit to 15 failed transactions. The problem this created is that limiting failed transactions in the Payeezy account is an all or nothing proposition at the account-level. Limits cannot be placed on individual transactions or users. This led to the problem of legitimate Coach's Oats customers not being able to process their credit card orders because the bad actors easily exhausted the 15-transaction limit within minutes. We had to find a way to beef up WooCommerce security and Payeezy wasn't going to provide any useful help.

The Dark Web

To understand what might be going on here, let's visit the dark web.

Eric Schmidt, Google's former CEO, estimated that the Internet consists of roughly five million terabytes of data. That's over five trillion megabytes. Google's web search has indexed about 200 terabytes of this data. That's a lot of data but it only comprises 0.004% of the entire thing. The other 99.996% percent of the internet is the Deep Web. The Dark Web is a subdivision of the Deep Web that search engines do not enter.

According to Wikipedia:

"The **dark web** is the World Wide Web content that exists on *darknets*: overlay networks that use the Internet but require specific software, configurations, or authorization to access.[1][2][3][4] Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location.[5][6] The dark web forms a small part of the deep web, the part of the Web not indexed by web search engines, although sometimes the term *deep web* is mistakenly used to refer specifically to the dark web.[7][2][8]

The darknets which constitute the dark web include small, friend-to-friend peer-to-peer networks, as well as large, popular networks such as Tor, Freenet, I2P, and Riffle operated by public organizations and

individuals.[6] Users of the dark web refer to the regular web as Clearnet due to its unencrypted nature.[9] The Tor dark web or **onionland**[10] uses the traffic anonymization technique of onion routing under the network's top-level domain suffix .onion."

When "private computer networks can communicate and conduct business anonymously without divulging identifying information", it doesn't take much to imagine the things that may go on in a place known as the "dark web". We've searched the dark web. It's not easy to navigate and requires special tools to access, but the things you can find for sale by Cybercriminals can be absolutely mind-boggling. The dark web is not a particularly pleasant or safe place to be.

For one, this is where Cyberthieves hold their bazaars and hawk their wares. Their wares are the ill-gotten gains from their orchestrated data breaches and hacks. Cyberthieves are everywhere. We all fight phishing spams and scams every day in our inboxes. As Cyberthieves get bolder, richer, and more brazen, they branch out beyond email. Some get into stolen credit cards. Some adapt to abuses with other forms of malware or ransomware. It's all about profits and cybercrimes provide substantial revenue streams.

And if Cyberthieves are seeking an access broker in the Cybercrime ecosystem to purchase a list of stolen credit card numbers, where do you think they'll find one willing to sell them merchandise curated from some hacker's data breach? On the dark web, of course. If they don't hack the list themselves, that is.

More than one cyberthief may purchase the same list of stolen credit card numbers from a broker on the dark web. Once the numbers are released, the next thing the cyberthief does is to test them to see which card numbers still have available credit so they can make a larger purchase or get cash withdrawals or do something else with them that only they know about. The first thief to find a valid credit card wins.

The easiest way to test credit cards is to breach a system like Coach's Oats and try to verify the card numbers through an eCommerce order process that uses a payment gateway with a vulnerability like Payeezy's. There's nothing wrong with the Coach's Oats website, mind you. It's as secure a WooCommerce site as any. There are untold numbers of systems on the web just like Coach's Oats that use Payeezy or similar gateways. Maybe yours is one of them.

If you run an online business and accept credit cards, pay attention to this particularly insidious scam. This white paper is written for you. Coach's Oats is not unique in how it conducts business on the web, or in its size as a small business. Cyberthieves are exploiting eCommerce systems as they are designed for everyday transactions. They are not installing malware and not hacking passwords or accounts. They are literally registering as your customer and robbing you blind in their pursuits with your own system's unpatched vulnerability. There are millions of small businesses in the United States that are comparable to Coach's Oats in their business profiles. Yours might be one of them; and everyone is a potential target. This means you, too! Can you afford an extra sudden expense that runs into the thousands?

Open Source Intelligence (OSINT)

Another thing that could be going on here is that the Cyberthieves aren't using the Dark Web at all but are relying on Open Source Intelligence or OSINT.

The term "open source" refers specifically to information that is available for public consumption.

According to U.S. public law, open source intelligence:

- Is produced from publicly available information
- Is collected, analyzed, and disseminated in a timely manner to an appropriate audience
- Addresses a specific intelligence requirement

The important phrase to focus on here is "publicly available."

If any specialist skills, tools, or techniques are required to access a piece of information like they are on the dark web, it can't reasonably be considered open source.

Information can also be considered open source if it is:

- Published or broadcast for a public audience (for example, news media content)
- Available to the public by request (for example, census data)
- Available to the public by subscription or purchase (for example, industry journals)
- Could be seen or heard by any casual observer
- Made available at a meeting open to the public

- Obtained by visiting any place or attending any event that is open to the public

That's a lot of information, a truly unimaginable quantity that is growing at a far higher rate than anybody could ever hope to digest.

Open source intelligence is most often used for ethical hacking & penetration testing or identifying external threats. Both use cases have legitimate purposes in the business world. However, if something is readily available to intelligence analysts, it's also readily available to threat actors. Threat actors use open source intelligence tools and techniques to identify potential targets and exploit weaknesses in target networks.

This is the main reason why so many small and medium-sized businesses get hacked each year. It isn't because threat groups specifically take an interest in them, but rather because vulnerabilities in their network or website architecture are found using simple OSINT techniques. They are easy targets.

Sometimes data breaches are found because someone left the details in an open source cloud storage location. Perhaps the data, including credit card numbers, was placed somewhere, and forgotten by a programmer or consultant for legitimate purposes such as a system upgrade or special project. Occasionally, breached data is just dumped to open source locations by hackers.

No matter where the Cyberthieves find their target information, whether from the dark web or open source intelligence, they pose an imminent threat to us that we must combat together.

THE INVESTIGATION

Coach's Oats orders display the IP address of the computer placing the order. IP addresses can be searched for the location where it is being used. Coach Nolan is the first who suggested that the Cybercriminals might be using a VPN. I'll prove later that Coach Nolan is right. After all, he's the only one I know that can solve a Rubik's Cube after looking at it for only a few seconds. He's usually ahead with his analytics and a great technology resource at the company, a prodigious partner who's easy to work with.

Using network tools available through the Wordfence firewall, I traced one of Coco's earliest IP addresses to a DSL line in a Philippines neighborhood. The tools at my disposal could only get me to the neighborhood level, but not to the house. If I could get to the house, maybe there would be someplace I can report the crime to as well. But reporting a crime to a foreign authority might prove difficult if not impossible. It would take more cybercrime fighting capabilities than I possess to even fully investigate, let alone make an arrest in this case, but who do I report it to, anyway? It's most definitely not the FBI's Cybercrime unit and I'm not aware of a global Cybercrime fighting authority. There's no place for me to go to report these Cybercriminals.

When I saw the IP addresses changing between orders, even for orders that appeared to be from the same person, I knew Coach Nolan was right about the VPN. I traced about a dozen additional order IP addresses, and they were located all over the world. Each time an order came in with a different IP address, the timing of the orders were just a few minutes apart. The only technology that I know of that can switch IP addresses that fast and maintain the internet connection is a VPN.

The fact that the cybercriminals are using VPNs to mask their trails means that finding them to report their activities to an appropriate authority is nearly impossible. At this point, there really wasn't anything more that I could investigate given my limited capability. It was time to move on to finding a solution to stop the activity in its tracks, if we could.

A Little About VPNs

There may be some of you reading this that may not know much about VPNs. They are marketed as tools you can use to protect your online privacy and, in most cases, require a subscription to access their services. As we've already learned from CoCo, they can be used for nefarious purposes as well because of the anonymity they provide.

VPNs are a very good tool when used for protecting your personal privacy. A VPN allows you to connect to the VPN network and conduct your internet activity through that connection. The IP address recorded by the site you're connected to with your browser is the IP address of the VPN server you're connected to through the VPN app. There's no way to trace your connection back to your actual location.

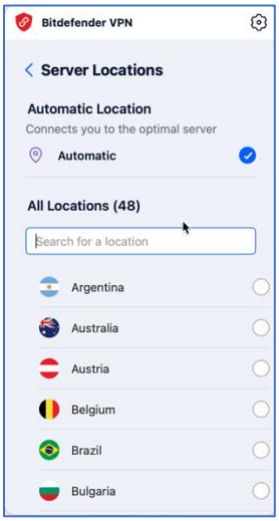


Figure 6: Bitdefender VPN Server List

We use the Bitdefender VPN in our development shop for all our Apple devices and Windows Virtual Machines. We do have one Windows laptop that we still use for testing code, but all our other devices are Apple. The Windows machine has Bitdefender on it as well.

If I want to change the IP address my electronic footprint is leaving behind on the internet, all I must do is click a button on my toolbar, connect to a different VPN server, and resume my online activity.

With the Bitdefender Premium VPN, I can connect to any of 48 secure locations around the world in seconds. Each one of those locations may have multiple VPN servers in its network that I can randomly connect to, with each presenting a different IP address.

VPNs are a great way to protect yourself when you're connecting to the Internet in a public place that has an open, insecure connection, which is most public access points. The innocent looking person sitting across the room from you in the café could very well be a Cybercriminal "sniffing" the WIFI connection for information they could leverage. Using the right equipment and software, they can read unencrypted communications or browser streams. How would you like to find out the hard way that someone sipping tea nearby is reading every bit of the information going over your internet connection? Why would you leave yourself so vulnerable? VPNs encrypt your communications with the VPN server, so you don't have to worry about someone "sniffing" out your signal.

COUNTERMEASURE PLANNING

The goal now is to stop the attacks and quench this fire. The countermeasure planning methodology we used is a standard team exercise where the Coach's Oats team, the Payeezy representative, and I shared frequent communications as a technical team with everyone staying in the loop. Since this aggressive of an attack is new to all of us, there are many suggestions and steps we try. Each step became progressively restrictive until I finally blocked every country in the world from accessing the site except the United States and Canada. (Countermeasure #4: The Nuclear Option) Since doing so, look at this log record:

Block Type	Detail	Rule Added	Reason	Expiration	Block Count	Last Attempt
IP Block	24.17.81.206	July 27, 2021 6:06 pm	Blocked by login security setting	Permanent	2	July 27, 2021 6:06 pm
Country Block	248 Countries (Entire Site)	July 23, 2021 9:36 am	Country Blocking	Permanent	4868	August 1, 2021 3:44 pm

Figure 7: Wordfence firewall log

This shows us that for the 10-day period from July 23, 2021, through August 1, 2021, 4,868 site access attempts from Countries other than the US and Canada were blocked by the firewall. That's an average exceeding 486 per day, a rate that remains fairly consistent.

I'd be thrilled to have more then 486 customers a day come to my business and want to spend their money, but if those 486 plus individuals are Cyberthieves, it takes on a whole new perspective for anyone that's being targeted. Coach's Oats doesn't sell product outside of the United States and Canada. What's your guess about who these blocked users are?

Coach Randy observed a threat about VPN access that I had already considered but decided to reserve. “If the cyberthieves are using VPNs,” Coach Randy asks, “what is stopping them from connecting to a VPN server in the United States or Canada and running the same scam?”

The answer is that there’s nothing blocking them and connecting to servers in the US or Canada could very well lead to another flood of failed orders and bad credit card transactions.

Our recommendation is to replace the Payeezy payment gateway with a different payment processor, just which one hasn’t been decided yet. The Coach’s Oats team is researching and testing alternatives.

We’ve managed websites that use Stripe, PayPal, and other bank related payment gateways such as Authorize.net. We’ve watched hundreds of thousands of dollars pass though these gateways for our clients. None of them have ever had an issue with this type of Cybercrime until this incident with Payeezy.

Every step we took was countered by the crooks and we implemented many safeguards. This is documented in the Countermeasures Implemented section. This type of attack has proven to be extremely difficult to thwart. The Countermeasures Implemented section explains the steps taken, plugins installed, and the results of each step’s success or lack thereof, as well as the counter-countermeasures the Cyberthieves used to neutralize our efforts.

We don’t know what we don’t know. We do know that we don’t have a thorough understanding of how this breach really occurred. Any conclusions we draw may prove to be purely anecdotal based on our experience and observations rather than empirical methodologies. We do have many questions though:

- Could the breach have been caused by a bot or series of bots?
- Are these attacks originating from one Cybercriminal or a Cybercriminal gang?
- Perhaps the shared server that hosts the site has been compromised. Are other sites in this shared environment experiencing similar attacks?
- Must we move to a more secure server environment?
- Should we engage an outside firm to perform penetration and intrusion detection to uncover other unknown vulnerabilities?
- Maybe we need to engage a more secure payment processor?

Ultimately, even if we do discover the answers to these questions, we are fighting the symptoms of the disease and not the disease itself. We don’t know the answers yet, but we are researching them. Our research may raise other unknown questions that need to be answered before we completely solve this mystery.

Whatever the outcome, we’ll update this white paper when we know more.

SITE PROFILE

Coach's Oats is a typical, well-managed WordPress-WooCommerce installation hosted on a SiteGround shared server. As the beneficiary of our basic care plan subscription, it receives the following essential services:

- Software Updates - WordPress Core and Plugins as needed
- Manual Website Check after Updates
- Daily Website Backups w/ Restoration
- Daily Security Monitoring with the Sucuri site scanner
- Daily Uptime Monitoring
- Daily Link Monitoring
- Database Optimization and Comment SPAM cleanup
- Monthly Performance Scan
- Email Support Ticket Desk
- 30-minutes of Support Task Time
- Monthly Maintenance Report w/ Site Analytics
- Access to our Exclusive Video Training Library

This is a very well-rounded support process to maintain the site in its optimal running condition.

Notice that a bullet point on this list mentions "Daily Security Monitoring with the Sucuri scanner". As a company, Sucuri has been around for a long time. They offer complete website security, protection, and monitoring through their cloud-based tools. We have hired them and recommended them in the past to help current and former clients whose sites have been hacked through weak admin passwords and the hackers either installed malware or defaced their content. While our site scanning process is automated,

Sucuri offers a free site scanning tool to the public. Try it as a first step if you think something may be wrong with your site or if you just want to see the information the scanner provides.

In addition to this daily Sucuri site scan, Coach's Oats uses the Wordfence Premium Endpoint Firewall and the Anti-spam Bee plugin to protect against comment spam. Wordfence does a lot to protect a site just with its free version. The Premium version adds Real-time IP Blacklist, Real-time Firewall Rule Updates, Real-time Malware Signature Updates, Reputation Checks, and Country Blocking, among some of its more advanced features. It also has a suite of network tools to help diagnose network issues, or in our case, trace an IP address to a neighborhood in the Philippines.

Let's keep something in mind here, this site security profile and plugins are the same or nearly the same as millions of WordPress-WooCommerce sites found in the wild. Why? Because these security plugins work well and protect sites globally. They do what they are designed to do and bring site owners peace of mind.

Even after we temporarily shut down the store to develop a permanent CoCo solution, hackers continued to try to breach the Coach's Oats Website. The first attempt was using a technique called Cross Site Scripting. This is where a hacker tries to breach your site by injecting executable code snippets through your URL. Wordfence immediately detected and blocked the attacks from causing any damage. The plugin also sent us this alert so we could in turn alert the Coach's Oats team that there was a hack attack in progress:

'This email was sent from your website "Coachs Oats" by the Wordfence plugin at Thursday 5th of August 2021 at 05:34:19 AM

The Wordfence Web Application Firewall has blocked 155 attacks over the last 10 minutes. Below is a sample of these recent attacks: August 5, 2021 12:30pm 64.37.231.158 (United States) Blocked for XSS: Cross Site Scripting in POST body: item_meta = jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(16281662.01957))//'

The actual email contained quite a few snippets of code the hackers were trying to inject into the Coach's Oats website, and they weren't all JavaScript based. Some of the injections were images that could contain scripts that execute when the image is viewed online. You could look at an image on the website and never know that it was executing a program to create a back door for the hackers or install malware on your site or the computer with which you are viewing your site.

155 attacks over a 10-munite period means the hackers were working at a rate of 1 attack every 4-seconds or less. But again, these hacker efforts were fruitless because they were immediately detected and blocked by the firewall.

Later on the same day as the URL Cross Site Scripting attack, the hackers tried to breach the site's WordPress comment system. Coach's Oats allows its users to respond to posts and recipes with their comments. The comments are generally nice and sometimes ask additional "how to" questions. This is how a comment system should work for a company. It helps build relationships and drive repeat business.

Occasionally a troll or spammer will post for their own purposes in a company's comment system. A troll is a wise guy that just likes to start trouble. It doesn't matter with whom or for what. This is how they get their jollies. Trolls and spammers leave spam comments. Spam comments are irrelevant to your content

and provide no value for your company. They frequently take the form of ads to purchase Viagra or Nike sneakers or some other products not suitable for a work environment. You can use your imagination here. Spam comments can be very bad!

Our daily client site maintenance dashboard shows us what comments are posted on a client's site since the day before. Visiting the dashboard is the first thing we do during our normal business day. If the comments are relevant, we leave them for the website owners to process.

Once in a blue moon, we see a troll comment posted. We must act on these because our task is to protect our client's site and reputation. Spammer ad content is stopped by Anti-spam Bee as they are posted. We never even see these anymore on any of our client sites that use this plugin.

The day after the URL Cross Site Scripting attack, our maintenance dashboard alerted us that a spam comment had been posted on Coach's Oats. We manually inspected the spam comment on the site and found it contained a single word that anyone with advanced programming knowledge would recognize. It was the evidence left behind of yet another Cross Site Scripting attack, but this time instead of trying to penetrate the site's URL, the hackers tried to breach the comment system but were stopped. If you can say anything about these hackers, they are persistent.

All the other plugins in use on the Coach's Oats site are standard WordPress and WooCommerce plugins designed to customize the site's functionality. All of them are scanned daily, function as designed, and are safe to use.

COUNTERMEASURES IMPLEMENTED

Countermeasure #1: Requests by Payeezy

Ever since the website went live, Coach's Oats has allowed guest checkouts for their purchasers. Guest checkout allows a customer to order and pay for their product without creating a WordPress account. It is a true convenience for eCommerce customers who may not be quite that tech savvy.

Because of the severity of the credit card verification breach, Payeezy agreed to refund some, if not all, of the bad transaction fees provided we implement steps that their engineering team recommended. Payeezy asked us to turn off guest checkout and force customers to create a WordPress account and authenticate their ID to pay for an order. They also requested that we implement reCAPTCHA on every page a customer accesses to submit information or orders.

Disable Guest Checkout

The whole idea of disabling guest checkout is to register or authenticate users before the checkout/payment process begins. This should give us at least a modicum of confidence that the user is legitimate. The first difficulty we encountered with this approach is that the Payeezy gateway displays its checkout payment screen before WooCommerce authenticates or registers a customer. This won't work as Payeezy had hoped because the Payeezy gateway is still open to the unverified. Somehow, we had to figure out how to swap the display order to have the registration/login screen show first. Luckily, there's a plugin for this: Force Authentification Before Checkout for WooCommerce.

Despite the incorrect spelling in the plugin's title for "Authentication", the plugin works. This free plugin has been installed over 4,000 times. Obviously, we're not the first business that has had to address this problem. First Countermeasure #1 challenge solved!

Enable reCAPTCHA

Google is making a concerted effort to roll out their reCAPTCHA Version 3 product to protect websites from fraud and abuse without creating friction. reCAPTCHA V3 uses an advanced risk analysis engine and adaptive challenges to keep malicious software from engaging in abusive activities on your website. In other words, reCAPTCHA V3 is a bot catcher.

Meanwhile, legitimate users will be able to login, make purchases, view pages, or create accounts and fake users will be blocked. Google's advanced risk analysis engine is located within their infrastructure, which means that every time a user logs into a site protected by reCAPTCHA V3, their details are passed to Google's servers for processing.

The first thing we tried to use is the reCAPTCHA V3 support features built into the Wordfence firewall.

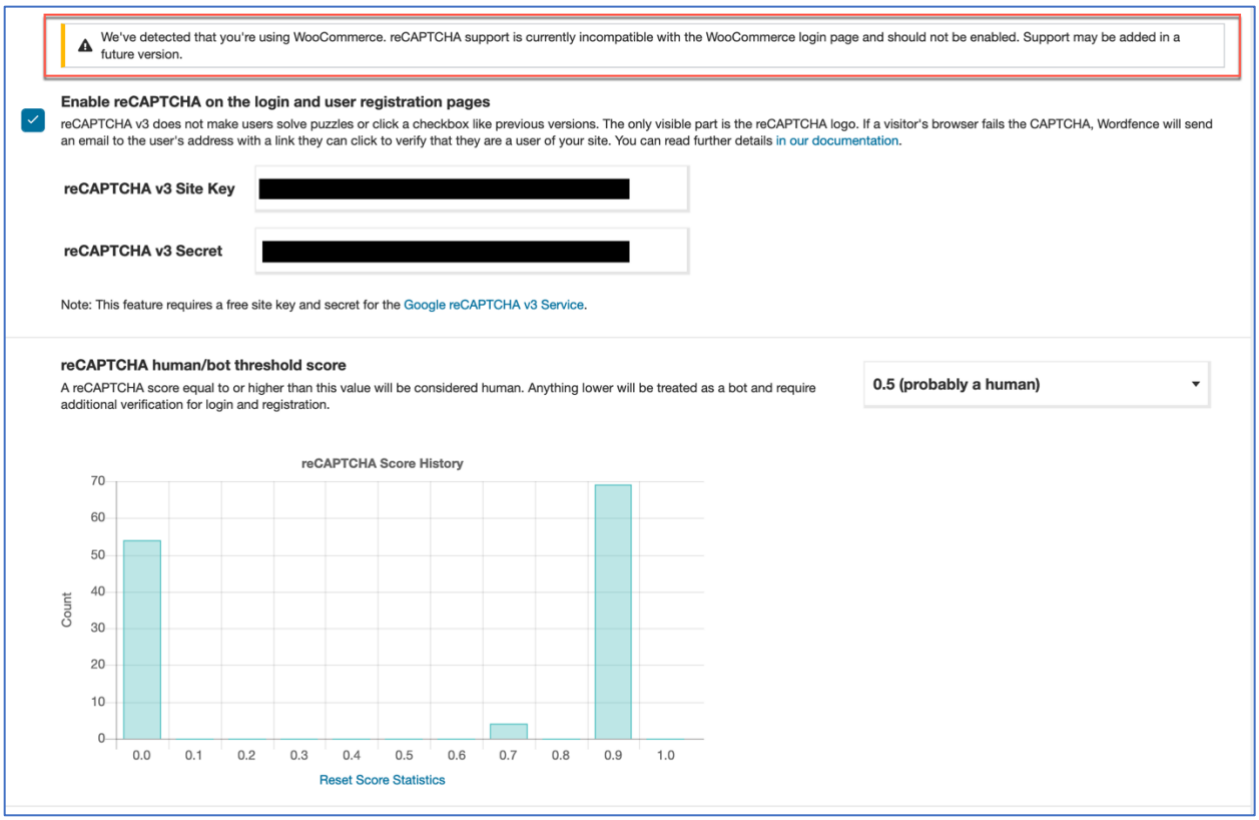


Figure 8: Wordfence reCAPTCHA V3 Support Setup Panel

Notice the message highlighted with the red box, "We've detected that you're using WooCommerce. reCAPTCHA support is currently incompatible with the WooCommerce login page and should not be enabled. Support may be added in a future version."

Wordfence's reCAPTCHA support only works with the standard WordPress user login and registration screens. We still needed to find a solution that works with WooCommerce, but we decided to leave this

Wordfence feature enabled since users can log into the site either through WooCommerce or the regular WordPress user login.

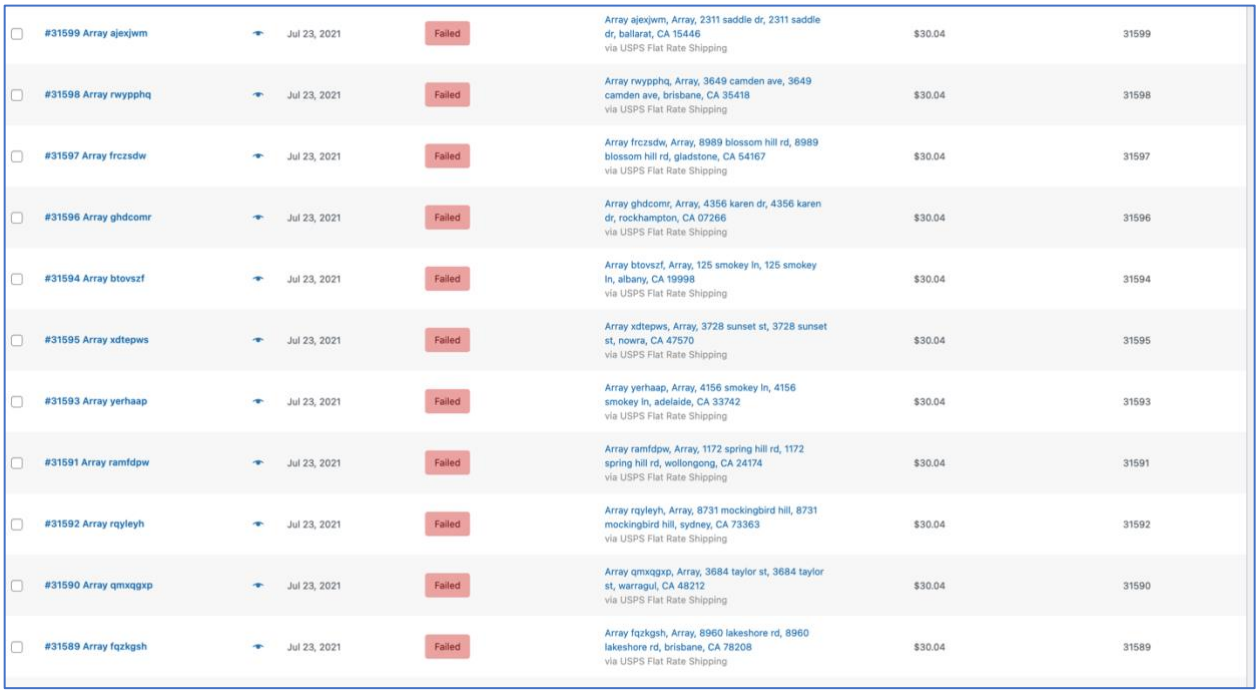
If you look at the reCAPTCHA Score History, in less than 2-weeks after this feature was enabled, 54 login attempts were by bots. These are shown in the 0.0 column. They were caught and blocked by Google. The 73 users in the 0.7 and 0.9 columns are real users. Admin logins are counted in these statistics.

To solve the WooCommerce reCAPTCHA challenge, we found this free plugin: Advanced noCaptcha & invisible Captcha (v2 & v3) (200,000+ installs). While this plugin can work across the board for WordPress and WooCommerce, we enabled it only for the WooCommerce registration and login screens so there was no conflict with Wordfence. They work together like a charm.

Countermeasure #1 Results

What are the results of implementing Payeezy's suggested fixes? Nada, zilch, nothing. It bombed! The bad credit card transactions were as bad or worse than they had been before the suggested "fixes" were applied.

Look at this order entry summary screen:



#31599 Array ajexjwm	Jul 23, 2021	Failed	Array ajexjwm, Array, 2311 saddle dr, 2311 saddle dr, ballarat, CA 15446 via USPS Flat Rate Shipping	$30.04	31599
#31598 Array rwypphq	Jul 23, 2021	Failed	Array rwypphq, Array, 3649 camden ave, 3649 camden ave, brisbane, CA 35418 via USPS Flat Rate Shipping	$30.04	31598
#31597 Array frczsdw	Jul 23, 2021	Failed	Array frczsdw, Array, 8989 blossom hill rd, 8989 blossom hill rd, gladstone, CA 54167 via USPS Flat Rate Shipping	$30.04	31597
#31596 Array ghdcomr	Jul 23, 2021	Failed	Array ghdcomr, Array, 4356 karen dr, 4356 karen dr, rockhampton, CA 07266 via USPS Flat Rate Shipping	$30.04	31596
#31594 Array btovszf	Jul 23, 2021	Failed	Array btovszf, Array, 125 smokey ln, 125 smokey ln, albany, CA 19998 via USPS Flat Rate Shipping	$30.04	31594
#31595 Array xdtepws	Jul 23, 2021	Failed	Array xdtepws, Array, 3728 sunset st, 3728 sunset st, nowra, CA 47570 via USPS Flat Rate Shipping	$30.04	31595
#31593 Array yerhaap	Jul 23, 2021	Failed	Array yerhaap, Array, 4156 smokey ln, 4156 smokey ln, adelaide, CA 33742 via USPS Flat Rate Shipping	$30.04	31593
#31591 Array ramfdpw	Jul 23, 2021	Failed	Array ramfdpw, Array, 1172 spring hill rd, 1172 spring hill rd, wollongong, CA 24174 via USPS Flat Rate Shipping	$30.04	31591
#31592 Array rqyleyh	Jul 23, 2021	Failed	Array rqyleyh, Array, 8731 mockingbird hill, 8731 mockingbird hill, sydney, CA 73363 via USPS Flat Rate Shipping	$30.04	31592
#31590 Array qmxqgxp	Jul 23, 2021	Failed	Array qmxqgxp, Array, 3684 taylor st, 3684 taylor st, warragul, CA 48212 via USPS Flat Rate Shipping	$30.04	31590
#31589 Array fqzkgsh	Jul 23, 2021	Failed	Array fqzkgsh, Array, 8960 lakeshore rd, 8960 lakeshore rd, brisbane, CA 78208 via USPS Flat Rate Shipping	$30.04	31589

Figure 9: Order Summary Screen Post Payeezy Requested Changes

The word "Array" is a programming term for a collection of variables. Every one of these failed orders is from a newly registered "customer" with the first name and an address that starts with the word "Array". The Cyberthieves are simply using the new process and registering as customers before fishing for good credit card numbers.

They are even somehow getting past reCAPTCHA V3's advanced risk analysis engine. Every one of these orders uses a different variation of a Google gmail address, which Google allows developers to do for testing purposes and not make it appear to Google email servers as spam.

Countermeasure #2: Fight the Fraud

The next battle in this war was delegated to the [WooCommerce Fraud Prevention Plugin] by the Dot Store.

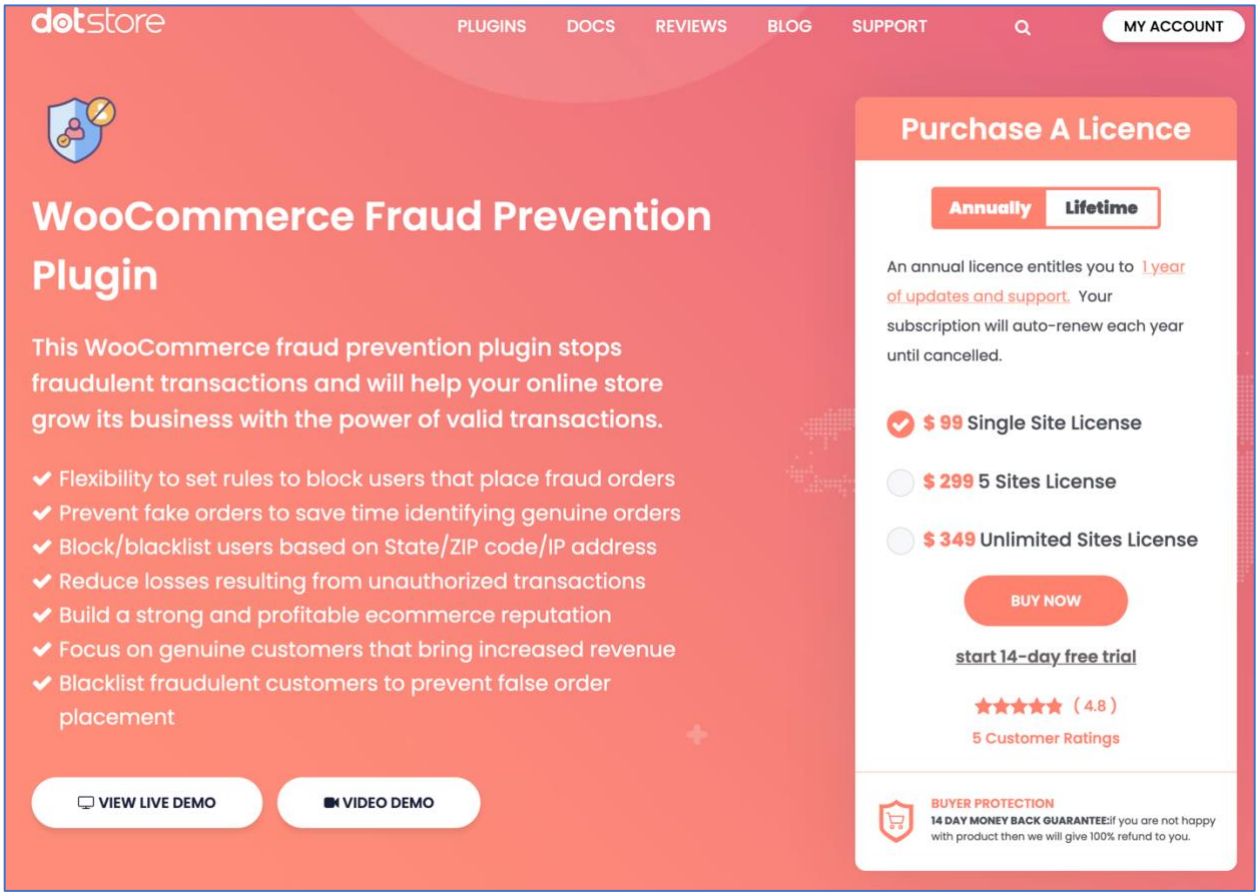


Figure 10: The Dot Store website

Reading through the materials seemed to us like it would do the trick. So, Coach's Oats decided to invest the $99 first year subscription fee to test its effectiveness. We've used Dot Store plugins on other sites for different reasons and they've always proven to work for their intended purpose. We had no reason to think otherwise this time.

Setting up the WooCommerce Fraud Prevention Plugin is largely a manual effort, though.

First, we define at what stage in the process we want the plugin to block fraudulent uses.

Next, we enter the first and last names and email addresses we want blocked. There is a section for blocking IP addresses, but we were already doing that in Wordfence and the Cybercriminals' use of VPNs circumvented IP blocking anyway.

Note the variations of the last name "Jimenez". These are alternate spellings CoCo used.

Countermeasure #2 Results

The name, email, and IP addresses changed fast and furiously after we blocked this dataset. The Cyberthieves sidestepped anything we tried with this plugin almost as fast as we implemented them. It did nothing to stop the credit card fraud in the Payeezy gateway. This plugin was an epic failure.

Countermeasure #3: Limit the Credit Card Failures

We knew that limiting the failed credit card transactions did not work at the Payeezy account level. However, we found another plugin that claimed it could limit failed gateway credit card transactions within WooCommerce itself. The free Woo Manage Fraud Orders plugin (2,000+ active installations) looked promising because its developer claimed,

"Another key feature of this plugin is that it tracks the number of fraud order attempts for payment gateways like Credit Card or Electronic Check. It blacklists the customer if the number of fraud attempts exceeds the limit set in the backend setting."

With the promise that this could limit the failed transactions in the Payeezy gateway, we installed and tested it.

The setup screen below defaults to 5 transaction attempts before it blocks a user. We set this initial value to 2. This caused a problem. If you recall, legitimate users sometimes enter credit card details incorrectly, which a couple of them did and they were blacklisted. We set the value back to 5.

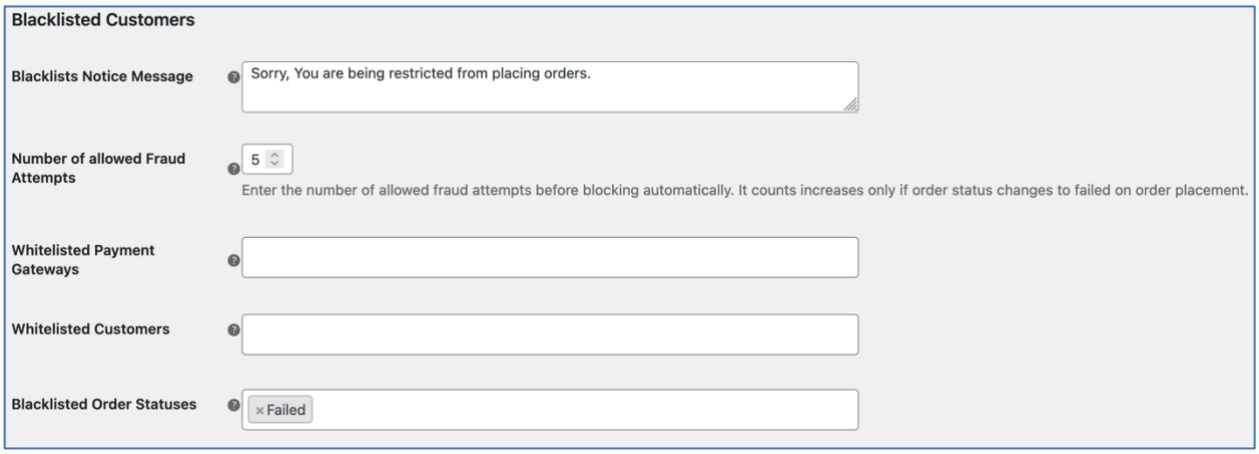


Figure 11: Woo Manage Fraud Orders Setup Screen (partial)

Countermeasure #3 Results

This plugin worked to a degree, but did it stop the fraud? No! After the Cyberthief account was blacklisted, the criminal created a new account with different details and ran fraudulent credit card verifications until they were blacklisted again after 5 more attempts. They did this repeatedly, effectively negating the protection this plugin provides.

Countermeasure #4: The Nuclear Option

With failure upon failure to stop these Cyberthieves amassing, the last thing we tried is the nuclear option, blocking every country in the world from accessing this site. You've already read about the results in an earlier part of this document. If you are not located in the United States or Canada and you try to reach the Coach's Oats site, you won't be able to. Wordfence country blocking works well, but it still doesn't stop the fraud.

CONCLUSION

The one thing we learned during this frustrating and challenging exercise is that if you collect credit cards online through your website and have a vulnerable gateway, Cyberthieves will find ways to exploit the vulnerability.

Truthfully, these days you don't even need to have a vulnerable website to become a victim. Just click on a link in an email you weren't expecting, even if it seems to be from someone you know or open an image or file that can execute scripts and you may be installing malware, key loggers, or some other software designed to steal your information onto your computer. You won't even know it's been done until you experience losses.

Please don't take unnecessary risks with your business and personal assets. If you own it and value it, there is a Cyberthief somewhere in the world that wants to take it from you. Be careful!

Key Takeaways

- There's a lot of money to be made in Cybercrime and it's getting much harder for Cybercrime fighting forces to stop it.
- Cyberthieves are persistent and will do everything they can to breach your site if they've targeted you
- With a vulnerable gateway, it's impossible to stop the fraud. You will bleed cash. Change to a more secure gateway or payment processor and keep your money for yourself.
- Keep your site updated and well maintained. Install state of the art firewalls and security plugins to detect and defend against most common breaches.
- Hire consultants that have the right level of experience with Cybersecurity. I mentioned several times about certain aspects of CoCo's attack that might be over my paygrade. Contact us for a free 30-minute, no obligation discussion, and if you need recommendations for higher paygrade security consultants, I'm happy to point you toward one.