# How Using WHOIS-Powered Tools Can Get You Ahead of E-Commerce Fraud

Posted on January 15, 2020

This coming holiday season, online retailers must remain vigilant as e-commerce fraudsters are certainly going to work harder than ever to take advantage of the throngs of shoppers sure to flock online.

The steady rise in e-commerce sales through the years makes online retailers lucrative targets for fraud. Last year's Black Friday sales total reached $6.2 billion, while the Thanksgiving online revenue reached $3.7 billion. Even Alibaba's recent Singles Day sales total reached $31 billion.

Predictions also state that the worldwide e-commerce sales revenue is poised to reach $4.9 trillion by 2021. While these figures are great for retailers, they also tell cybercriminals they have a lot to gain from preying on e-commerce sites.

Fraudsters always choose victims that would earn them the highest profits. The fact that many online retailers do not have effective security measures in place makes them easy targets with big payoffs. In Amazon's case, the delay in checking returned goods proved faulty (as we will thoroughly discuss later in this post).

Cybercriminals also take advantage of the online retail frenzy every peak shopping season. They are likely to bank on the fact that retailers would focus on fulfilling as many orders as possible without checking if transactions are valid. In 2017, for instance, the number of fraud cases grew twice as much as the e-commerce sales volume.

Like any other cyberthreat, it is best to stop fraud before transactions are completed. Proactive solutions such as an email verification API can help detect anomalies by ensuring that the email addresses provided by shoppers are valid.

This post delved into what reports have dubbed "the biggest Amazon scam in Europe" and how email verification could help prevent potential fraud damages. It also provides more information on the various scams online retailers need to be wary of and how these can be addressed.

### Table of Contents



## The Biggest Amazon Scam in Europe

Retail giants like Amazon are no strangers to fraudulent transactions. Given their massive customer base, its sellers and customers are automatically prime cybercrime targets.

### The Scam

What has been dubbed the biggest Amazon scam in Europe to date took advantage of Amazon's sales return process. A 22-year-old identified as James Gilbert Kwarteng from Spain successfully ordered several items from Amazon, which he then sold online. Apart from earning back the money he spent, he also managed to trick Amazon into reimbursing him for supposed product returns. Instead of sending back the goods purchased, however, he sent resealed boxes full of dirt.

Amazon's return policy states that customers who are not happy with their purchases can return these within 30 days and get either refunds or replacements (in cases where the goods were not in satisfactory condition). Those who opt for a refund typically get this in 1–2 business days.

That's how Kwarteng got away with the scam (at least for a while). He made sure that the weights of the boxes matched those of the products he ordered. And since returned items are not always opened or checked upon receipt, the scam may have gone unnoticed for a certain period. We can surmise that the perpetrator was well-versed with Amazon's return policies, which allowed him to find a weakness to take advantage of.

### The Scammer's Take

Kwarteng and his unnamed associate swindled a total of $370,000 from this scam alone, which did not require them to use sophisticated malware or break into Amazon's network. Kwarteng even reportedly established his own company Kwartech using his profits from the scam.

The case seems surreal, and if a giant retailer such as Amazon could fall prey to such an incident, it's not hard to imagine how other retailers stand to lose should they suffer the same fate. And this is not the only type of fraudulent activity retailers need to be wary of, there are tons more.

## Various E-Commerce Fraud Types to Watch Out For

### Chargeback Fraud

In this type of scheme, customers buy products with their credit cards and then, later on, claim that they did not conduct the transactions. They cite identity theft, and so the card provider ends up paying for the goods purchased by a supposedly unauthorized user.

## Identity Fraud

Cybercriminals are known for using stolen credit card credentials to make card-not-present transactions. These credentials are by-products of breaches that are sold in underground markets or the Dark Web. In some cases, they even go the extra mile and sell payment card clones using the stolen credentials.

## Card Testing Fraud

They say there is no honor among thieves, and that is true for cybercriminals. Some first test the stolen credentials they bought to make small purchases. If these go undetected, they then move on to making big purchases. More advanced hackers use bots to generate card verification values (CVVs) when these buy goods by using active credit card numbers. This tactic helps them avoid having ties to the illicit purchases.

Overall, fraud subjects online retailers to various consequences apart from incurring financial losses due to lost sales. If they cannot disprove a customer's false claim in a chargeback fraud case, for instance, they end up not just losing a sale but also paying back the customer for something he/she did buy and most likely kept. Online merchants are slated to lose $31 billion from chargeback fraud alone by 2020.

E-commerce platform owners can, however, thwart fraud with the help of tools such as Email Verification API, IP Geolocation API, and WHOIS API. The next section shows how.

# E-Commerce Site Owners Can Fight Back with Email Reputation API and Other Domain Research and Monitoring Tools

### Email Verification API

Most, if not all, e-commerce sites require customers to use a valid email address as their username. Email Verification API is an effective means to verify the existence of an email address. It can:

- Check if the email address conforms to Internet Engineering Task Force (IETF) standards using a complete syntactic validation engine.
- Determine if the email address uses a misspelled version of a popular service provider's domain, along with other common fake address patterns.
- Ascertain whether the email address is provided by a known disposable email address provider such as Mailinator, 10MinuteMail, GuerrillaMail, and at least 2,000 more similar entities.
- Verify the email address against a database of Domain Name System (DNS) mail exchange (MX) records.
- Make sure the email address exists and can receive messages using a Simple Mail Transfer Protocol (SMTP) connection via email-sending emulation techniques.
- Check if the email address can receive messages from any email address.

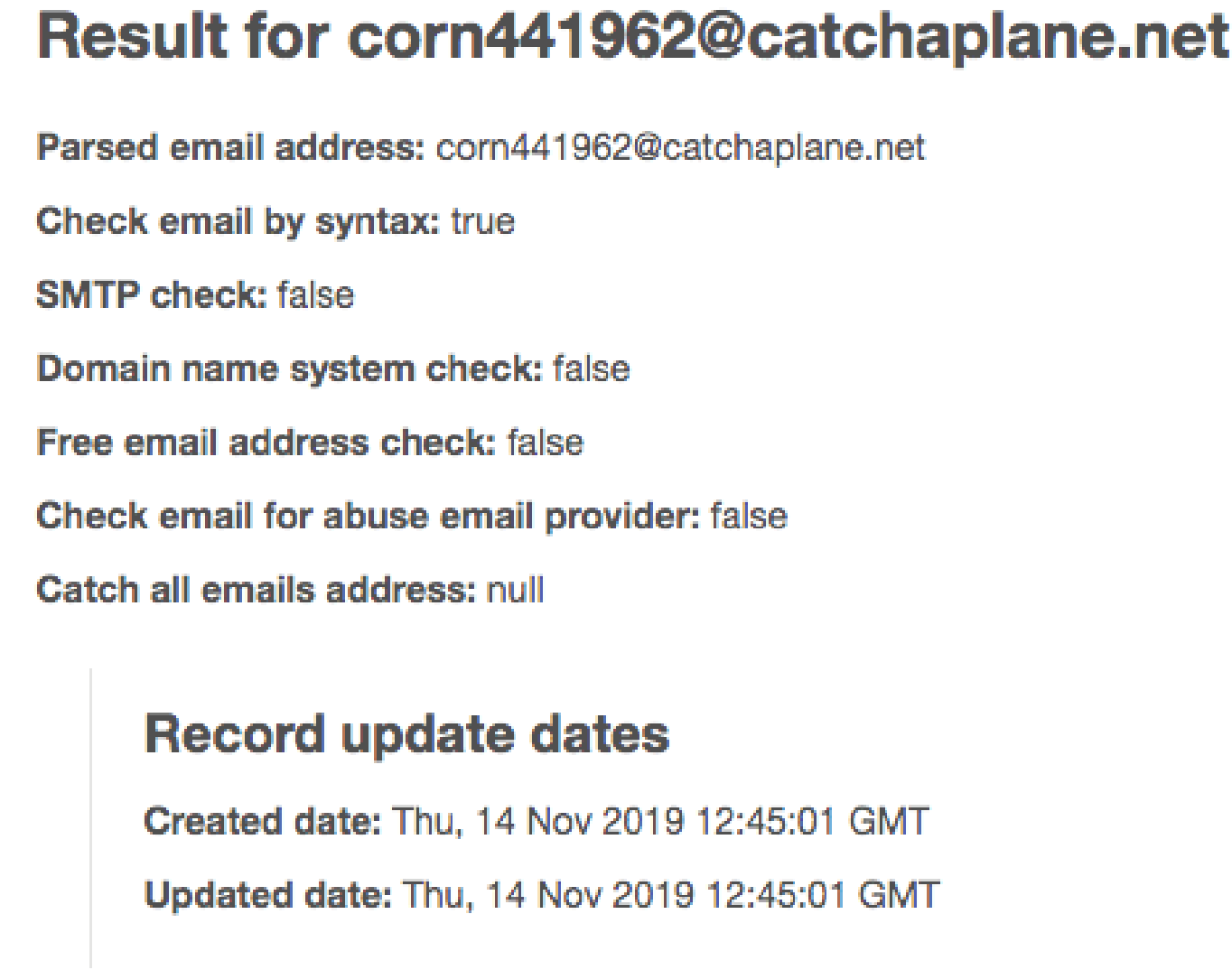
These checks occur in a matter of seconds but they still provide an additional layer of protection for online retailers who wish to ensure that all of their customers are who they claim to be.

Fraudsters frequently use disposable email addresses in their attacks, which they abandon once the transactions are completed. Integrating the API into an e-commerce system and configuring it to run automatic email verification checks can lessen a retailer's chances of dealing with unscrupulous individuals.

Here is how the tool works:

- Let us say that a visitor registers at your e-commerce site. He used the email address corn441962@catchaplane[.]net. If you integrated Email Verification API into your registration form, it should automatically query the email address.

- Our manual query returned the following results:



# Result for corn441962@catchaplane.net

**Parsed email address:** corn441962@catchaplane.net

**Check email by syntax:** true

**SMTP check:** false

**Domain name system check:** false

**Free email address check:** false

**Check email for abuse email provider:** false

**Catch all emails address:** null

## Record update dates

**Created date:** Thu, 14 Nov 2019 12:45:01 GMT

**Updated date:** Thu, 14 Nov 2019 12:45:01 GMT

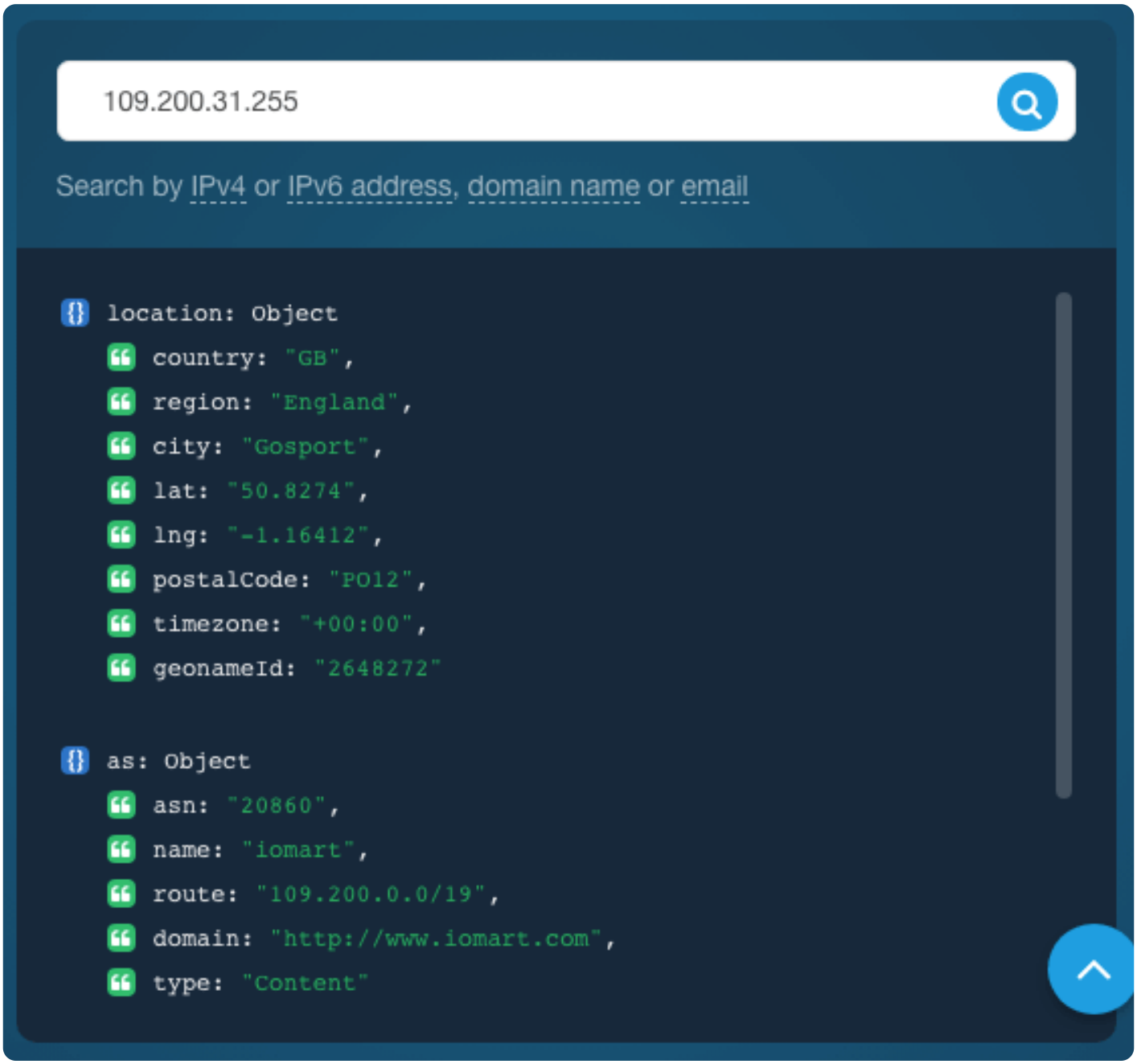
- As shown, the email address does not exist and does not have a valid domain. If configured to reject nonexistent email addresses or domains, the visitor's registration to the site should be rejected. This simple email verification process already weeds out potential fraudsters from the get-go.

### IP Geolocation API

Another useful tool for e-commerce site owners is IP Geolocation API. It can serve as an additional verification layer to ensure that the customer making purchases is who he/she claims to be based on his/her geolocation. Upon checkout, an IP Geolocation API-enhanced form can be configured to cross-check the user's geolocation with the billing address stated in his/her registration record. If they do not match, the site administrator can initiate additional verification steps.

Here is a demonstration of how the tool works:

- Let us say that your frequent customer John Doe resides in Dallas, Texas. Because he typically purchases goods from home, his IP address is pretty consistent (i.e., 165.231.212.16). But someone with a different IP address (i.e., 109.200.31.255) just logged in to his account to purchase goods. A query for 109.200.31.255 returns this result:


109.200.31.255
Search by IPv4 or IPv6 address, domain name or email
location: Object
country: "GB",
region: "England",
city: "Gosport",
lat: "50.8274",
lng: "-1.16412",
postalCode: "PO12",
timezone: "+00:00",
geonameId: "2648272"
as: Object
asn: "20860",
name: "iomart",
route: "109.200.0.0/19",
domain: "http://www.iomart.com",
type: "Content"

- Your IP Geolocation API-enhanced system can be configured to reject the transaction because the user's geolocation clearly does not match John Doe's billing address. This approach provides an additional layer of protection, not just for the retailer but also for its loyal customer.

## WHOIS API

If, like Amazon, you are unfortunate enough to have been scammed in the same way, you may wish to file a case against the perpetrator. However, building a strong case requires evidence.

We heard that Kwarteng (the Amazon scammer) established a company to sell the goods he was able to steal essentially. That company is known as "Kwartech." Supposing you were one of his victims, you can investigate his domain with WHOIS API.

We queried the domain kwartech.com on the tool and got this result:

**Parsed domain name:** kwartech.com

**Domain name extension:** .com

**Estimated domain age:** 89 day(s)

**Contact email:** abuse@godaddy.com

**Created date:** Fri, 16 Aug 2019 14:46:22 GMT

**Updated date:** Fri, 16 Aug 2019 14:46:23 GMT

**Registrar name:** GoDaddy.com, LLC

**Registar Internet Assigned Numbers Authority ID:** 146

**WHOIS server:** whois.godaddy.com

**Domain EEP status codes by ICANN list:** clientTransferProhibited clientUpdateProhibited clientRenewProhibited clientDeleteProhibited

**Custom field name 1:** RegistrarContactEmail

**Custom field value 1:** abuse@godaddy.com

**Custom field name 2:** RegistrarContactPhone

**Custom field value 2:** +1.4806242505

**Custom field name 3:** RegistrarURL

**Custom field value 3:** http://www.godaddy.com

The domain was anonymously registered, but its age coincides with the period when the scam was pulled.

## Domain's registrant

**Name:** Registrant State/Province: Select a region

**State:** Select a region

**Country:** SPAIN

**Country code:** ES

## Administrative contact

**Country:** SPAIN

**Country code:** ES

## Technical contact

**Country:** SPAIN

**Country code:** ES

The country matches Kwarteng's as well. It is thus a pretty good bet that kwartech[.]com is worth investigating further. (Note: we wouldn't recommend to visit or interact with the site unless you have good reasons to believe it's safe or are an experienced investigator.)

## 'Tis the Season to Be Vigilant

For years, the retail industry has been a favorite target of fraudsters and cybercriminals. E-commerce fraud that comes in various forms — mimicking online retailers' websites to steal from its unsuspecting customers, abusing return policies as in the featured case, disputing legitimate transactions, and others — all translate to losses for retailers. Those whose sites are spoofed end up losing customer confidence and trust. Others who succumb to giving refunds just to retain customers despite suspicions lose substantial amounts.

Online retailers can combat the hazards of e-commerce fraud with the right set of tools and security measures. They can integrate tools such as Email Verification API and IP Geolocation API into their e-commerce platforms so they can spot potential fraudsters upon site registration or before checkout. By adding at least two layers to their customer verification processes, they will be able not only to protect their own interests but those of their customers as well.

Apart from using various solutions, we also recommend the following best practices for online retailers:

- Keep your systems and applications patched at all times. Attackers can exploit weaknesses in hardware and software to gain access to your network.
- Make sure your site URLs do not point to rogue servers by performing regular checks on your DNS infrastructure. Redirects to malicious sites could land your site in a blacklist and thus prevent customers from reaching them.
- Decommission unused sites and pages so these cannot be hacked and used by attackers.

Make sure these do not have ties to your authoritative nameservers.

- Encrypt credit card numbers and other personally identifiable information (PII) that are stored in your systems. That way, even if those get stolen, attackers will not be able to use them.
- Be wary of customers placing bulk orders within a short period. They could be cybercriminals maxing out the limits on stolen credit cards before those get cut off.
- Carefully scrutinize customers who use different credit cards despite coming from a single IP address.
- Beware of different customers who use the same credit card number. One of them could be a cybercriminal armed with a payment card clone.

Regardless of its size, your e-commerce site is subject to fraud. But with tools that provide real-time information about site visitors, it is possible to detect the bad guys in various ways.