

# Fraud Prevention in Ecommerce Report 2021/2022

Best Practices Into Stopping Fraud to Convert More Orders and Increase Revenue



Endorsement partner:



Key media partner:



# Nethone

## Evolution of Fraud Attacks: How New Strategies Emerge, Stacked on Top of Tried and Tested Methods



At Nethone, **Aleksander** bridges the gap between the tech and business teams, translates complex and technological ideas into clear gains with client needs turned into tangible product developments. Additionally, he loves to dive deep into exploring new areas and opportunities for Nethone to deliver better results for our customers. When not fighting fraud, he can be found reading with a self-brewed third-wave coffee next to him or bouldering.

Aleksander Kijek ■ Chief Innovation Officer ■ Nethone

The rise of ecommerce's share of global retail sales – from 14% in 2018 to 19% in 2020 due to the effects of COVID-19 lockdowns – has likewise led to an increase in global fraud rates. This is in part down to a new group of online shoppers not fully aware of the dangers of the internet. They are perfect targets. Fraudsters use a bag of tricks based around *social engineering* (an act that influences a person to take an action that may not be in their best interest) to get what they want from them.

*Phishing* remains a prominent scam method, where cybercriminals fool victims to divulge sensitive information. Emails are sent, garnering fear and urgency, enticing people to click on a malicious link. They are directed to what appears to be a legitimate service to make an outstanding bill payment or update details. If successful, the account falls under the control of the fraudster.

Similar techniques include *vishing* (eliciting information or action over the phone) and *SMiShing* (using SMS to do the same). By utilising sophisticated tools to spoof caller ID (but not always), a direct call or SMS appears to be sent from the victim's own bank or another service, requiring urgent action. By influencing an individual to install a remote desktop programme (RDP, linking two networked computers) to supposedly fix a problem, a fraudster gains account access. Surprisingly, the main aim is not to steal money: the bigger prize can be scans of ID documents saved on the victim's device, used to assume a real identity to open multiple new accounts, launder cash, and take out loans.

### Two-factor authentication (2FA) is not so strong

In what for a long time has been standard for authenticating online transactions and preventing phishing, 2FA appears to provide adequate protection. It is based upon two levels of security: a password (something you know), and an authentication code often received via SMS on a phone (something you own). Unfortunately, fraudsters have upped their game so much that 2FA provides little more than a false sense of security.

Cybercriminals can defeat 2FA using the Murena and NecroBrowser toolkit. Developed by researchers Michele Orru and Guiseppe Trotta, the aim was to highlight that anti-phishing strategies can be compromised. Previous deep technical knowledge and many tools were required to defeat 2FA – attackers needed to have their phishing sites function as proxies, forwarding requests to legitimate services and deliver responses in real time. The aim was to gain access to valid browser cookie sessions, but they had to be used quickly before expiring.

The Murena and Necrobrowsers toolkit automates the entire process, bypassing 2FA using a reverse proxy solution, capturing login credentials and valid session cookies. Necrobrowser uses the gathered cookies, instructing a set of dockerized Chrome browsers to ensure the stolen sessions remain active, allowing a fraudster to use the target account until they are discovered. →

A simpler method to get around 2FA is *SIM swapping*. Through phishing and/or social engineering, a fraudster obtains a victim's details, using them to contact their mobile service provider. Impersonating the victim and feigning the loss of a phone, they attempt to convince the provider to port the number to a new SIM. If successful, all incoming calls/messages (including verification codes) will be sent to the fraudster's phone.

### ATO fraud attempts in ecommerce will only increase

Cybercriminals are always trying to stay one step ahead of anti-fraud actors aiming to thwart their efforts. Fraudsters are becoming increasingly crafty, deploying a hybrid of new, tried, and tested techniques to achieve account takeovers (ATO).

To combat fraud, the European Union introduced PSD2/SCA (Payment Services Directive/Strong Customer Authentication) regulations, requiring merchants to incorporate multi-factor authentication for online transactions. This has improved anti-fraud measures, and rather than going up against advanced security, many fraudsters choose to focus attention on ATO. The methods are easier than you think, which is why ecommerce merchants need to take effective counter-measures.

### Fraudsters try to beat anti-fraud by behaving like a normal customer

Once an account has been acquired, a fraudster will aim to act similarly to the original account holder in order to 'warm up the shop'. This process requires time and patience.

The fraudster's first steps are to analyse the account's purchase history, delivery address, payment methods etc. This is followed by browsing online shops and adding similar previously purchased products to the shopping cart. Returning days later, adding more goods, making the purchase and leaving reviews will seem natural. Some fraudsters, in a very nonchalant manner, will also contact

customer services to engage in conversation to create a bond with an ecommerce merchant. Eventually, unwanted items will then be removed from the cart with only the desired items purchased. This can go on indefinitely until the fraud is discovered.

### Advanced anti-fraud solutions based on exhaustive end-user session profiling and machine learning can prevent attacks


Such effective attacks highlight why merchants have begun to take their users' behaviour seriously and that rule-based anti-fraud systems can be ineffective against evolving attacks. The answer to these problems is to deploy advanced anti-fraud solutions based on behavioural biometrics, digital fingerprinting, backed up by AI/machine learning models. This is precisely what Nethone provides. Our integrated solution effectively differentiates genuine customers from fraud actors in real time and in a non-invasive manner. Global fraud threats and techniques are evolving, but so too are the solutions.

[Click here for the company profile](#)

**Nethone**

nethone.com

**Nethone** is a machine learning-based fraud prevention SaaS company that allows online merchants and financial institutions to holistically understand their end-users — also referred to as 'Know Your Users' (KYU) in industry parlance. With its proprietary online user profiling and ML technologies, Nethone is able to detect and prevent payment fraud, account takeovers, with unrivalled effectiveness.

Company		Nethone	
		Nethone is a machine learning-based fraud prevention SaaS company that allows online merchants and financial institutions to holistically understand their end-users – also referred to as 'Know Your Users' (KYU) in industry parlance. With its proprietary online user profiling and ML technologies, Nethone is able to detect and prevent payment fraud, account takeovers, with unrivalled effectiveness.	
Background information			
Year founded	2016		
Website	https://nethone.com/		
Target group (Merchants/ecommerce; PSP/acquirers; SMBs; Banks/FS; Corporate; Fintech; Telecom)	Merchants/ecommerce Banks/FS PSP/acquirers Fintech		
Supported regions (US; Europe; Middle East; APAC; Africa; LATAM; India; China; Global)	US, Europe, Middle East, APAC, LATAM, India		
Contact	Hubert Rachwalski von Reichwald, CEO, hubert.rachwalski@nethone.com or contact@nethone.com		
Company's motto	Detect fraud with our Know Your Users solution		
Member of industry association and/or initiatives	MRC, About Fraud, VTEX , Nissho, CeFPro		
Core solution			
(Fraud/risk management and decisioning platform; Customer authentication; Identity verification; Behavioural biometrics; Data provider and intelligence; Chargebacks management; Bot risk management; KYB/Merchant onboarding; KYC)	Fraud/risk management and decisioning platform Customer authentication Identity verification Behavioural biometrics Chargebacks management Bot risk management KYB/Merchant onboarding KYC		
Core solution/problems the company solves	Nethone prevents online businesses from card-not-present fraud, provides them with real-time recommendations to optimise their business decisions and help online lending companies with credit scoring. Nethone also prevents account takeover, promo abuse, refund abuse, synthetic ID, alternative payment methods (APM) thanks to behavioural biometry (5000+ attributes about each user gathered by Nethone Profiler) and machine learning.		
Technology			
(On-premise; Cloud enabled; Native cloud; Hybrid)	Native cloud		
Data input			
Identity verification	proprietary capability	third party	both
Identity document scanning			
Video scanning			
Personally Identifiable Information (PII) validation		x	
Small transaction verification	x		
Email verification			x
Phone verification			x
<div>View company profile in online database</div>			
FRAUD PREVENTION IN ECOMMERCE REPORT 2021/2022   COMPANY PROFILES			

Social verification			x
Credit check		x	
Compliance check	x		
Online authentication	proprietary capability	third party	both
Behavioural biometrics	x	x	x
Physical biometrics			
Device fingerprinting	x		
Geo-location			
Remote access detection	x		
Mobile app push			
3-D Secure 2.0			
Hardware token			
One-time passwords			
Knowledge-based authentication			
Intelligence	proprietary capability	third party	both
Abuse list	x	x	x
Monitoring	x		
Address verification			
Credit bureau			
Information sharing			
Data ingestion/third-party data			
Stateless data ingestion and augmentation	x		
Methodology			
Machine learning (Rule-based; Supervised ML; Unsupervised ML; Hybrid)	Hybrid		
Decisioning			
(Manual review; Case management; Decision orchestration)	Case management Decision orchestration		
Chargeback management			
(Chargeback dispute; Guaranteed fraud protection)	N/A		
Business model			
Pricing model	Fixed fee for model (re)training and maintenance + per transaction/operation		
Fraud prevention partners	Ekata, Ethoca, Paay, Verifi, IP intelligence, BIN databases		
Year over year growth rate	2017 - 100% 2018- 772% 2019 - 89% 2020 - 66%		
Number of employees	79		
Future developments	Deeper technical user profiling		
Customers			
Customers reference	Farfetch, Azul, VTEX, Grover, Booksy, Vivus, Wonga, ING, PKO Bank Polski, Mokka, Straal, Bitcan, eSky, Polish Airlines LOT, Nissho, epag, Ramp Network, Smartney (Oney Bank Group)		

# Nethone

## Detect fraud with our Know Your Users<sup>TM</sup> solution

```
1275 $return = array();
1276 $result = mysql::query("SELECT * FROM image_date ORDER BY shot_date DESC");
1277
1278 while($day = mysql::fetch($result)) {
1279     $studio_list = array();
1280     $shots_result = mysql::query("SELECT DISTINCT(studio) as studio, COUNT(*) as count FROM image WHERE shot_date = '$day'");
1281     while($shots_result = mysql::fetch($shots_result)) {
1282         $studio_list[] = $shots_result->studio;
1283     }
1284     $studio_list = array("studio" => $studio_list->studio, "count" => $studio_list->count);
1285     $studio_list = $tmp_studio_list;
1286     $return[$day->shot_date] = $day;
1287 }
1288 return $return;
1289 }
1290
1291 static function day_images_list($date, $studio) {
1292     global $global_studio_list;
1293     if(!in_array($studio, $global_studio_list)) die("error studio");
1294     $date = mysql::escape($date);
1295     if(mysql::count("image_date", "shot_date = '$date'") != 1) die('date not found');
1296     $date = intval($date);
1297     $result = mysql::query("SELECT image_id as image_id FROM image, image_date WHERE image_date.id=image.id AND image_date.shot_date = '$date'");
1298     while($image = mysql::fetch($result)) {
1299         $image->copyright = metadata::get_copyright($image->image_id);
1300     }
1301     return $result;
1302 }
1303
1304 $result = mysql::query("SELECT image_id as image_id FROM image, image_date WHERE image_date.id=image.id AND image_date.shot_date = '$date'");
1305 while($image = mysql::fetch($result)) {
1306     $image->copyright = metadata::get_copyright($image->image_id);
1307 }
```

Recognize and reject non-human interactions of bots and scripts, suspicious behavior, anomalous device configuration and fraudulent tools. Use Machine Learning to identify recurring users and prevent ATO.



Advanced Fraud Solution - prevent account takeover (ATO) and chargebacks with our integrated system using behavioral biometry, digital fingerprinting backed up by Machine Learning models.



Frictionless Checkout - improve UX while being PSD2 SCA compliant and fully secure using our passive anti-fraud solution.



Increased Sales Conversion - let your business grow with improved fraud protection, frictionless UX and positive customer reviews.

Schedule a demo at: [www.nethone.com](http://www.nethone.com)  
or write to us: [contact@nethone.com](mailto:contact@nethone.com)

Nethone