Press release
Warsaw, 16.04.2019

Experts Warn: New Fraud and Chargeback Thresholds Require Revision of Risk Management Strategies

- **From October 1st, 2019, online merchants accepting credit and debit cards will have to comply with new, stricter anti-fraud regulations imposed by Visa – the world's largest card organisation. The monthly compliance thresholds are to be lowered from 1% to 0.9%.**
- **Companies operating in fraud-prone industries need to revise their risk management strategies immediately.**
- **Merchants should work closely with Payment Service Providers (PSPs) to develop effective chargeback control mechanisms and fraud prevention measures.**

From October 1st, 2019, online merchants accepting Visa cards will have to comply with stricter anti-fraud regulations. All monthly compliance thresholds (including the ones established by VCMP Standard program) will be lowered from 1% to 0.9%, which will affect all entities accepting cards issued under Visa brands, especially companies from high-risk industries. Michał Jędraszak, CEO of Straal and Hubert Rachwalski, CEO of Nethone join forces to explain what consequences the new regulations might bring for merchants and how to get ready for the upcoming changes.

The new fraud and chargeback monitoring policy poses challenges especially for merchants operating in industries such as travel (OTAs, Airlines), online video games, betting and gambling, nutraceuticals, pharmaceuticals, dating or adult entertainment as well as those offering digital goods – often balancing on the brink of the threshold even under the current, more forgiving regulations.

At the moment, the VFMP's (Visa Fraud Monitoring Program) monthly compliance thresholds are set up to a 1% fraud-dollar-to-sales-dollar ratio. Similarly, the VCMP's (Visa Chargeback Monitoring Program) ones are established to a 1% ratio of disputes-to-sales-transaction count. These figures relate to MATCH (Member Alert to Control High-Risk Merchants) – a system designed by Visa to monitor businesses experiencing excessive fraud attacks as well as encourage them to incorporate measures targeted at preventing fraudulent transactions. Merchants get listed on MATCH after exceeding the thresholds consecutively for several months.

Merchants who are currently dangerously close to the 1% threshold, after the changes will fall into chargeback monitoring programmes with a danger of joining the high-risk merchant category. Hubert Rachwalski, CEO of Nethone, explains how to minimize this threat.

The new, stricter thresholds do pose a challenge to merchants but there is a way to overcome this problem. The starting point is redefining one's risk management strategy: the updated one might make use of deep profiling of users, which aims at understanding fully customers in digital channels, based on accurate fraudster identification. Only KYU performed in real time combined with innovative PSP's processing that use this kind of sophisticated analytics will enable high-risk entities to continue growing – comments Mr. Rachwalski.

The tightened threshold will increase the number of penalties for merchants who unsuccessfully set their risk management strategies. Straal's CEO Michał Jędraszak translates the threat into specific numbers.

These fees range from $50 per chargeback up to $75.000 of a monthly non-compliance fee, depending on the threshold exceeded and non-compliance severity. For, for instance, a digital goods merchant processing high volume of low-value transactions or a company selling high-value digital or semi-digital services such a situation might lead even to bankruptcy – explains Mr. Jędraszak.

Both experts emphasize that merchants should now work closely with PSPs to develop effective risk management strategies, capable of matching the tightened monitoring thresholds. Moreover, the new regulations will also affect acquiring banks as their fraud thresholds will be lowered, too. As a result, this party will also get involved in working on more effective fraud prevention.

First of all, the key question is about the responsibility for effective fraud prevention. Is this burden on the merchant's shoulders or maybe on the PSP's? Should a merchant search for third party providers of FDP solutions on their own or expect such support from their payment gateway? At Straal, we believe that in most cases the latter makes more sense – explains Michał Jędraszak. *While in low-risk industries a set of simple anti-fraud rules should do the job, in industries balancing on the brink of the threshold detection of fraudulent behaviour requires more sophisticated tools and smooth cooperation between the gateway provider and the anti-fraud solution* – adds Mr. Jędraszak.

Efficient fraud detection and prevention relies on collecting and crunching huge amounts of meaningful data.

To protect a business against fraud, one has to establish effective data gathering processes. It's crucial to collect quality, meaningful data that will help to understand the context of fraudulent transactions – explains Mr. Rachwalski. – *It is recommended to* *gather detailed user data as well as rich information about transactions processed by the PSP. Joining forces at this stage translates into better fraud prevention results, meaning more accurate detections and fewer false positives.*

As Machine Learning (ML) is the most efficient way to spot differences between legitimate users and fraudsters with high accuracy and in real time, collecting big amounts of meaningful data and providing its smooth flow between systems is paramount. The key principle of ML is the more data it gets, the more accurate predictions it gives.

The more data a model receives, the better results Machine Learning it generates. In this context, it means better fraud prevention thanks to more accurate predictions. However, training a model takes time – it is worth commencing the process now so that it is perfectly ready when the new regulations take effect – says Michał Jędraszak.

Both experts agree that a merchant approaching the current 1% fraud threshold should instantly contact their PSP and ask what is going to change once the new regulations come into force. It may be also necessary to agree on a new risk management strategy or just find a PSP cooperating closely with a quality fraud-fighting partner.

***

Straal is an international provider of payment, optimization and fraud prevention solutions for future-minded businesses. The company offers a comprehensive suite of products that make accepting digital payments easier, as well as more effective and secure. Straal enables accepting one-off and recurring payments carried out by customers with credit and debit cards of all major organizations, initiating SEPA Direct Debit cycles and more. Thanks to Straal, customers can pay in currencies of their choice (over 150 options), using their preferred desktop and mobile platforms, while merchants can effectively maximise their transaction approval rate and mitigate risk. Founded in 2017, the company is headquartered in Warsaw, Poland. Learn more: www.straal.com

Nethone is the global leader in AI-driven KYU (Know Your Users) solutions that help enterprises from all around the world convert cyberthreats into well-informed, profitable decisions. From world-class fraud prevention up to account takeover detection based on advanced behavioural biometrics, Nethone services simultaneously protect bottom lines and elevate profits of forward-looking businesses. Founded in 2016 by experienced data scientists, security experts, and business executives, Nethone is one of the tech fastest-growing companies in Central Europe. Since the beginning of March 2019 Nethone is a part of the world's most prestigious travel tech acceleration programme headquartered in Silicon Valley – Plug-and-Play. More details on: www.nethone.com

Contact

Olgierd Borówka
Marketing & PR Manager
olgierd.borowka@straal.com
+48 784 624 480