Risk Management for Third Party Payment Networks

van Driel, Willem; Hernandez Ganan, Carlos; Lobbezoo, M; van Eeten, Michel

Publication date
2016

Document Version
Final published version

Published in
Proceedings of Workshop of Economics of Information Security 2016

Risk Management for Third Party Payment Networks

Willem van Driel
Adyen
1011 DJ Amsterdam
The Netherlands
Willem.vanDriel@adyen.com

Carlos Gañán
Delft University of Technology
2628 BX Delft
The Netherlands
C.H.G.HernandezGanan@tudelft.nl

Maikel Lobbezoo
Adyen
1011 DJ Amsterdam
The Netherlands
Maikel.Lobbezoo@adyen.com

Michel van Eeten
Delft University of Technology
2628 BX Delft
The Netherlands
M.J.G.vanEeten@tudelft.nl

***Abstract*—The payment industry has been characterized by a small number of players that operate the schemes for the facilitation of credit and debit card payments. Over the years, various initiatives have been taken in order to increase competition and hence cost efficiency within the industry. One of the latest efforts is the introduction of Payment Service Directive II (PSDII) within the European Union. PSDII requires banks to open up their services to Third Party Payment (TPP) networks. TPP networks make use of banks' payment initiation services for e-commerce transactions, creating an alternative next to credit and debit card payments. However, just like in the card networks, payment fraud is not absent in TPP networks. Fraud manifests itself in non-payments: authorized payments that do not get settled. In this paper we first analyze the ecosystem dynamics of the TPP network by examining the role of each actor involved. By leveraging one year of transaction data from the TPP network, we estimate the prevalence of non-payments. Finally, we evaluate a preventive and reactive risk management strategy. The latter strategy comprises of a non-payment recovery process — sending the consumer a reminder of the due amount — and proves to be surprisingly effective. Additionally, we have evidence that combining both strategies into a continuous risk management process can yield even better results. As non-payment in the TPP network has similarities with chargebacks in the card network, we believe that our approach can also enhance risk management in the card network.**

I. INTRODUCTION

Although the e-commerce payment process may look simple from the consumer's perspective, a lot of complexity is hidden behind the scenes. Over the past decades an entire financial sector has emerged to deal with this complexity: the payment industry. The industry is currently characterized by a small number of players, like MasterCard and Visa, that operate the schemes for the facilitation of credit and debit card payments [1]. This dominant position is not solely the result of the direct usage of credit and debit cards for e-commerce payments, but also because many other payment methods such as provided by PayPal, Apple Pay and Android Pay make use of credit and debit card schemes for their payment processes.

Over the years, various initiatives have been taken in order to provide an alternative to the card network: the part of the payment industry that makes direct or indirect use of the card schemes. Alternatives are believed to enhance competition and lead to more efficiency within the payment industry. Some believe that blockchain technology will provide this alternative [2]. Others believe that the way forward is making use of real time bank transfers, as already mentioned by Anderson in 2012 [3]. In order to stimulate the latter development in the European Union, the European Parliament has adopted Payment Serviced Directive II (PSDII) on the 8th of October 2015 [4]. PSDII requires banks to open up by providing third parties access to account information (XS2A) and payment initiation services (PIS). In practice this implies that, with the consent of the consumer, a third party can access the consumer's bank account to obtain account information (e.g. transaction history) and initiate bank transfers on the consumer's behalf.

In this paper we focus on third parties making use of PIS. PSDII refers to this new ecosystem as the Third Party Payment (TPP) network. The TPP network provides the payment industry the opportunity to develop payment methods that circumvent the card schemes. The introduction of PSDII has led to some early entrants into this potential growth market, such as Swedish Trustly [5] and German Sofort [6]. Outside of the European Union TPP networks are also on the rise, such as Walmart's CurrentC [7] in the United States and Australian Post's POLi Payments [8] in Australia. In this paper we focus on the European Union's TPP network, however our results are believed to be indicative of TPP networks in general.

One of the main risks for merchants in the card network is the presence of chargebacks. After a card

payment has been made, the consumer holds the right to reverse his payment for a limited period of time — e.g. when the goods or services are not satisfactory [9]. This creates a financial risk for the merchant, as the goods and services are often already delivered at the moment the chargeback is issued. Chargebacks that are issued for non-legitimate reasons are associated with fraud. For many merchants losses due to fraud have a significant impact, sometimes threatening their complete business model [10]. Over the past decades, an extensive amount of research has been dedicated to risk management for card networks, which has resulted in a decreased relative chargeback exposure for the industry [11].

Although payments in the TPP network should not be subject to chargebacks, practice has shown that payments can be reversed. Research into risk management for TPP networks however, is practically non-existent. This paper aims at filling this gap, by examining risk management strategies from the merchant's perspective — as it is typically the merchant who ends up absorbing the financial loss of reversed payments. From this point we will refer to reversed payments in the card network as chargebacks and reversed payments in the TPP network as non-payments. We use this differentiation because although reversals in both networks share characteristics, they do not occur for the exact same reasons — as will be elaborated on in Section II.

The contribution of this paper is three-fold. (1) First, we analyze the functioning of the TPP network. This enables us to differentiate non-payments from chargebacks. (2) Second, we present a detailed analysis of the non-payment characteristics using one year of transaction data from the TPP network. The results indicate that non-payments tend to concentrate during the weekend, during the night, at specific types of merchants and specific types of issuing banks. (3) Finally, we design strategies to manage the risk of non-payments and empirically apply and evaluate their effectiveness. The results indicate that whereas preventive risk management strategies are cost effective for the card network, the TPP network might be served better with reactive strategies — i.e., accepting to a certain extent that non-payments occur and mitigate their impact afterwards. We see opportunities for future research into optimizing the strategies, designing new strategies and combining preventive and reactive strategies for the development of a continuous risk management process.

The remainder of the paper is structured according to the three contributions of our research. In section II we present how the TPP network is organized and elaborate on the similarities and differences between chargebacks in the card network and non-payments in the TPP network. In section III we describe the characteristics of one year of transaction data from the TPP network and analyze patterns for the occurrence non-payments. In section IV, we propose two risk management strategies to mitigate the impact of occurrence of non-payments and apply them in practice. Finally, we discuss the results of our research in section V and conclude upon its main findings in section VI.

II. THIRD PARTY PAYMENT NETWORK

A. The Network

A TPP network consists of "any agreement or arrangement that involves the establishment of accounts with a central organization by a substantial number of providers of goods or services who are unrelated to the organization and who have agreed to settle transactions for the provision of the goods or services to purchasers according to the terms of the agreement or arrangement" [12]. According to the US Code of Federal Regulations, payment is guaranteed in the settlement of such transactions. In practice, however, this settlement does not always occur.

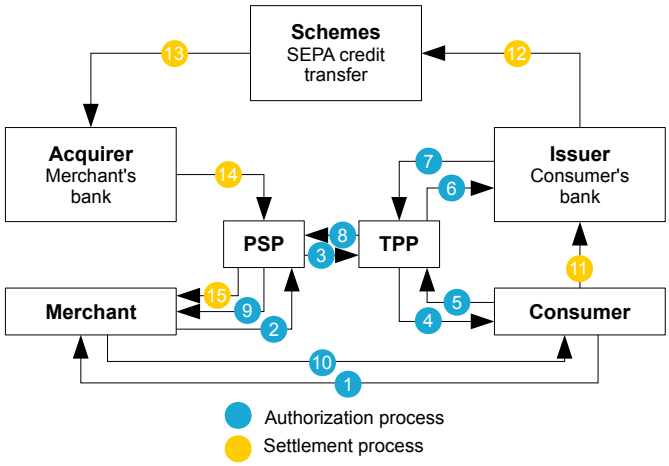

Figure 1. TPP network and its payment process

The TPP network, as visualized in Figure 1, has its similarities with the card network. To represent the TPP network, we have created an extended version of the four corner model that is typically used to represent the card network [9]. Just like the card network, the TPP network consists of the merchant and the acquirer

(the merchant's bank); the consumer and the issuer (the consumer's bank); the schemes which are used for the communication between the acquirer and issuer; and, optionally, a Payment Service Provider (PSP) to connect the merchant to multiple acquirers. Also just like in the card network, the payment process in the TPP network is separated in two main processes: (1) authorization and (2) settlement. The authorization process is a flow of information in which the merchant gets the confirmation whether the funds will be transferred — i.e., the settlement will take place. With this confirmation, which is typically provided (near) real-time, the merchant can already deliver his goods or services to the consumer, as the merchant has the guarantee that the funds will be transferred at a later stage. The settlement process in which the funds are actually transferred takes place after authorization and can take up to a few days to be completed. The authorization process in the TPP network consists of the following 10 steps:

1) The consumer indicates to the merchant the chosen TPP to carry out the payment;
2) The merchant connects with the PSP to initiate the payment;
3) The PSP sends the payment initiation to the TPP;
4) The TPP asks the consumer for the credentials of the online banking environment;
5) The consumer submits the credentials to the TPP;
6) The TPP connects with the issuer's online banking environment and initiates the payment;
7) If the payment initiation is successful, the issuer sends an approved authorization to the TPP. If the initiation is not successful, the issuer sends a rejected authorization;
8) The TPP sends the authorization response to the PSP;
9) The PSP notifies the merchant of the authorization response;
10) The merchant notifies the consumer of the authorization response.

The settlement process in the TPP network, which can only take place after an approved authorization, consists of the following five steps:

11) The consumer's funds are captured by the issuer;
12) The issuer sends the funds to a clearing house in the format of the SEPA credit transfer scheme [13];
13) The clearing house sends the funds to the acquirer;
14) The acquirer sends the funds to the PSP;
15) The PSP redirects the funds to the merchant.

Despite the similarities between the payment processes in the TPP network and the card network, there are two main differences. First, in the TPP network the schemes are not used for the authorization process. Instead, the TPP is responsible for obtaining the authorization from the issuer directly. Second, the TPP network makes use of the standard European Union's bank transfer scheme, the SEPA credit transfer [13], for the settlement process, rather than one of the card schemes. Because of these two differences, payment processing in the TPP network has no dependency on the schemes of the card network. As such the TPP network provides the payment industry with the attractive possibility to develop payment methods that circumvent the card schemes. A drawback is that, due to its infancy, the TPP network might be more prone to safety and security issues, as emphasized in section 1.9 of the European Commission's PSDII impact assessment [14].

B. Chargebacks Versus Non-Payments

Both chargebacks in the card network and non-payments in the TPP network typically result in a financial loss for the merchant as he does not receive the consumer's funds. Despite this similarity, the main difference between chargebacks and non-payments resides in their moment of occurrence in the payment process. A chargeback typically takes place after both the authorization and settlement have been completed. This implies that although the funds are already transferred to the merchant, the consumer can still claim them back. A non-payment in the TPP network can not take place after the settlement has been completed. A non-payment is a payment for which an authorization was provided by the issuer, however, the issuer has not released the funds for the settlement.

Chargebacks initiated for non-legitimate reasons are typically associated with fraud. But when could a non-payment be associated with fraud? To answer this question, we first look at the origin of fraudulent chargebacks in the card network, for which Kahn and Roberds [15] distinguish three different modus operandi. First, they identify *new account fraud* where the fraudster obtains someone's identity to apply for a new account. Chargebacks occur if the victim reverses payments that are made using his identity. Second, they mention *existing account fraud* where the fraudster initiates a transaction using someone's account illicitly. If the legitimate account holder reverses the payments, this results in chargebacks. At last, they identify *friendly fraud* in

which the fraudster orders goods and/or services using his own account and later denies having placed the order.

How would these modus operandi translate to the TPP network? For new account fraud, the fraudster would have to open a bank account, and know how to play the system in order to obtain authorizations that would not result in a settlement. For existing account fraud, the fraudster would have to obtain access to someone's online banking environment, and play the system in a similar fashion. Both these modus operandi seem rather ineffective for the fraudster, because of the high costs to deploy them in the TPP network rather than in the card network — applying for a bank account, or obtaining access to someone's two-factor secured online banking environment is typically more costly than applying for a credit card or stealing someone's credit card details. This can also be observed by the higher losses resulting from card fraud than from online banking fraud [10]. That leaves us with friendly fraud as one of the more viable modus operandi for fraud in the TPP network. However, when a non-payment occurs, it is unclear what its underlying reason is. The consumer might not be aware of the fact that his transaction was not settled, but he could also be exploiting vulnerabilities in the TPP network to generate unauthorized overdrafts. Before elaborating on this difference we first present attributes that increase the likelihood of occurrence of non-payments — regardless of whether they are fraud related or not — in the subsequent section.

III. NON-PAYMENT CHARACTERISTICS

For this study, we analyzed one year of transaction data from the TPP network, spanning from from 1/8/2014 till 1/8/2015 and collected by Adyen, a globally active PSP. It consists of close to 3.5 million transactions. As the data originates from the PSP, the transactions and attributes that are captured are limited to those that the PSP sees. In other words, the data consists of all TPP transactions for 767 merchants which use Adyen as their PSP. Table I presents general characteristics of the data.

The data considers transactions initiated from within the DACH-region (Germany, Switzerland and Austria), a selection we have made because these are the countries where the TPP network is most prevalent. It is worth noting the presence of the large number of issuers even though the transactions were initiated in just three countries. It implies that there are a minimum of 598 different issuing banks operating within these markets. This can be explained by the decentralized nature of the banking sector within these countries [16]. As will be elaborated on later in this section, most non-payments are concentrated on a small subset of these issuers.

Table I. General characteristics of the data

Descriptive	**Value**
Number of transactions	3,472,209
Number of non-payments	10,008
Number of merchants	767
Number of consumers	996,854
Number of issuers	598

Let us define the non-payment ratio (NPR) as *the number of transactions that resulted in a non-payment over the total number of transactions*. Over the analyzed period the NPR is about 0.003 equaling 0.3%. This is substantial when considering that the chargeback ratio in the card network for the similar set of merchants over the same period of time was around 0.005 equaling 0.5%.

We identified several attributes that increase the likelihood of occurrence of non-payments. Table II presents an overview of the attributes that influence this likelihood the most. The attributes are categorized to be either related to the transaction itself or to be related to one of the stakeholders of the TPP network, as displayed before in Figure 1. Analyzing the attributes per stakeholder enables us to identify where in the ecosystem encompassing the TPP network high concentrations of non-payments reside. In the following subsections we describe the patterns that are present in each category.

Table II. Attributes that influence the non-payment ratio

Category	**Attribute**
Transaction	Day of week, hour of day
Merchant	Name
Consumer	Country, device type
Issuer	Name, settlement delay

A. Transaction

An increased non-payment ratio was observed for transactions that were initiated in and around the weekend, as visualized in Figure 2. The NPR is almost twice as high on Saturdays ($\text{NPR}_{Sat} \simeq 0.0037$) than on Thursdays ($\text{NPR}_{Thu} \simeq 0.0021$). Similarly, we observed an increased ratio for transactions initiated during the night. At its peak (i.e., around 3am) the NPR is more than twice as high as during its low at noon. At its peak NPR is about 0.006, which implies that 0.6% of all transactions initiated at that time result in a non-payment. Overall, the NPR during non-business hours is

higher. This might be caused by the fact that some banks only operate their settlement systems during business hours, indicating that the occurrence of non-payments can actually be a double spending problem.

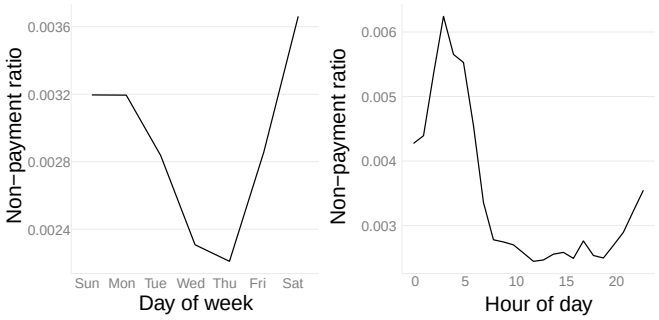

Figure 2. Non-payment ratio per day of week and hour of day

B. Merchant

For the merchant-related attributes, the data revealed that there is a concentration of non-payments on a small selection of the merchants. The top ten merchants that generated most non-payments account for 74% of all non-payments while accounting for 58% of all transactions. Most of these merchants offer gaming or gambling-related services. These services are characterized by frequent payments of individual consumers, for example to purchase new gaming or gambling credit.

C. Consumer

For the consumer-related attributes we observed an increased NPR for transactions initiated from mobile devices. The NPR for consumers using their tablet or computer is comparable. The NPR also seems to be influenced by the country the transaction was originated from. The NPR for transactions originated from Switzerland is more than four times higher than transactions originated from Germany and Austria.

D. Issuer

For the issuer-related attributes, the data revealed that there is a concentration of non-payments on a small selection of the issuers. The top five issuers that generated most non-payments account for 73% of all non-payments while only accounting for 28% of all transactions. This indicates an even higher concentration of non-payments on specific issuers than on specific merchants. Also, we found a relation between the issuer's average settlement delay — i.e., the time between the authorization and the settlement — and the NPR, as visualized in Figure 4.

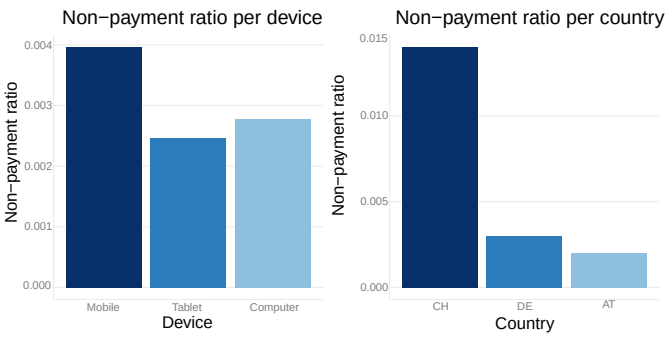

Figure 3. Device type and country versus non-payment ratio

Non-business days are excluded from the settlement delay, as banks typically only settle on business days. The dotted line represents the average NPR over the whole dataset of 0.003.

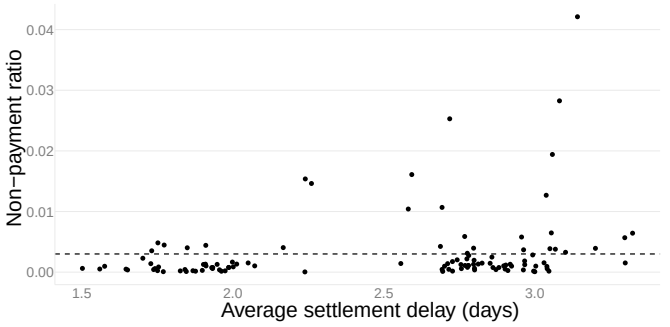

Figure 4. Settlement delay versus non-payment ratio

From Figure 4 it can be observed that the issuers with the highest NPRs are also the ones that have the highest average settlement delays. The highest NPR for an individual issuer equals 0.042 implying that 4.2% of the issuer's authorized transactions are not settled.

Looking at the non-payment characteristics it can be observed that there are possibilities to fundamentally improve the functioning of the TPP network. For example, issuers can improve their settlement processes to lower the NPR outside business hours. It is questionable, however, whether all stakeholders in the ecosystem around the TPP network share similar incentives to deploy these potential systemic improvements. The stakeholder who ends up with the financial loss of non-payments, the merchant, is also one of the stakeholders who has least influence on the deployment of these improvements. To deal with this challenge, we present risk management strategies that the merchant can deploy in the subsequent section. In practice, we assume that these strategies will

be executed by the PSP, as the PSP has access to more and more diverse data than the individual merchant, increasing the efficiency of the strategies. As the PSP can be regarded as an *umbrella organization* acting on behalf of the merchant [9], we presume their incentives to deploy improvements to be aligned.

IV. RISK MANAGEMENT STRATEGIES

As mentioned in the introduction, research into risk management for TPP networks is practically non-existent. In order to deal with the risk of the non-payments we have designed two risk management strategies.

The first strategy is deployed before authorization of a transaction and tries to utilize historical transaction data to estimate the likelihood that the observed transaction will result in a non-payment using a random forest classifier. If the likelihood surpasses a predefined threshold, it is blocked.

The second strategy is deployed after authorization, and only if no settlement has taken place — i.e., a non-payment occurred. The strategy encompasses a non-payment recovery process in which the consumer is requested to pay the due amount, as the funds have not been received by the merchant. We explore both strategies in more detail and examine their effectiveness.

A. Preventive Strategy: Non-Payment Prediction

In order to prevent chargebacks in the card network, a wide variety of statistical machine learning techniques is applied by the various actors involved in the payment process. Among the available techniques, supervised machine learning methods (e.g., random forest) are most commonly used [17]. Because of the similarity between chargebacks and non-payments, and because of the observed patterns in non-payment occurrence as presented in previous section, a random forest classifier also seems suited for the prevention of non-payments in the TPP network. The classifier can be used to identify subsets of transactions where the NPR is significantly higher than in other subsets.

In order to enhance the performance of the classifier we decided to use a subset of the transactions based on the observed concentration of non-payments on specific issuers and merchants. We selected the intersection of transactions of the top ten merchants and top five issuers as presented in previous section. This reduced the size of the dataset to a total of $586,438$ transactions of which $5,747$ resulted in a non-payment. As a result of using this subset, the NPR in the dataset equals 0.0098 or 0.98%.

For the classifier, we made use of the attributes as presented in Table II. We add derived attributes that can serve as an indicator of fraud, inspired by work of Bhattacharyya et al. [18]. The underlying assumption is that fraudsters tend to clean an account as quick as they can, once they have access. This involves making multiple and/or high value transactions in a short time interval. The attributes are displayed in Table III.

Table III. Attributes used as indicator of fraud

Attribute	Description
Is first transaction	Indicator whether transaction is first transaction of consumer
Time since last transaction	Time since last transactions from consumer
Cumulative amount on same day	Cumulative amount consumer has spent on transaction day
Cumulative count on same day	Cumulative number of transactions consumer has initiated on transaction day

Besides the challenge of selecting attributes to train the classifier, we were confronted with imbalanced data. In order to reduce the imbalance in the training set, various sampling methods can be used. As argued by Bhattacharyya et al. [18], random oversampling of the minority class, in our case the transactions that resulted in a non-payment, can enhance the performance of the classifier. Therefore, the training set is comprised of a random selection of 50% of all transactions with non-payments. The training dataset is extended with a random selection of normal payment transactions, in such a way that the training set consists of 50% non-payments and 50% normal payments.

B. Reactive Strategy: Non-Payment Recovery

As the reactive strategy we designed a non-payment recovery process. In order to deal with the non-settled transactions, we regarded these as accounts receivable. For the transactions that resulted in a non-payment, we asked the merchant to contact the consumer to inform him about the due amount. Following this, and with the consumer's consent, as obtained by the merchants, we initiated a SEPA direct debit [19] to capture the due amount from the consumer's bank account. If this direct debit did not bounce, and no reversal[1] of the SEPA

[1]SEPA direct debits [19] can also be reversed, either by the consumer or by the issuer. The reasons for these reversals differ from the ones in the card and TPP networks. To avoid increasing complexity we decided to leave the analysis of these reasons out of the paper's scope.

direct debit occurred, we would consider the due amount to be successfully recovered. Seen this way, the non-payment recovery process works as an alternative way of settlement for a transaction that was already authorized. Please note that for our research the contact with the consumer was established by the merchants themselves, and not by the researchers or the PSP.

C. Strategy Evaluation

The results of the application of the two strategies are presented in Table IV. For each strategy we have included two types of measures: the direct costs of the application and the risk mitigation. The direct costs of the random forest classifier include the costs of false positives, calculated by summing the transaction value of the blocked transactions which, in reality, did not result in a non-payment (false positives). The direct costs of the non-payment recovery process include the issuer fees calculated by summing the transaction costs of processing the SEPA direct debits. As the non-payment recovery process is deployed after authorization, there are no false positives and no costs of misclassification.

Both strategies come with development and maintenance costs, for which we include simple estimates. The development costs for the random forest are estimated 1/2 FTE[2] and the maintenance as 1/4 FTE. For the non-payment recovery process these costs are estimated to be 1/4 and 1/2 FTE respectively, because there is less automation and more manual labor. The risk mitigation for each strategy is calculated as the total transaction value of non-payments that were (1) prevented or for which (2) the due amounts were recovered, divided by the total transaction value of the non-payments.

Table IV. Direct costs and risk mitigation per strategy

	Preventive strategy *Non-payment prediction*	**Reactive strategy** *Non-payment recovery*
Direct costs		
False positives	$ 5,578,864	$ 0
Issuer fees	$ 0	$ 32,378
Development	$ 75,000	$ 37,500
Maintenance	$ 37,500	$ 75,000
Risk mitigation	25%	76%

It can be observed that the direct costs of the non-payment recovery process are lowest, and its risk mitigation is highest. Given this information, it is obvious that the non-payment recovery process is more effective than the non-payment prediction. However, given the fact that the NPR may vary over time, we want to incorporate this variability in our comparison of the two strategies. To accomplish this we make use of the Return On Security Investment ($ROSI$) model, as introduced by Sonnenreich, Albanese and Stout [20], which can be used to evaluate security investment decisions. In contrast to other approaches, Sonnenreich et al. [20] do not split the costs used for determining the $ROSI$ model further into different types of costs. The $ROSI$ is determined by:

$$ROSI = \frac{risk\ exposure \times risk\ mitigated - solution\ costs}{solution\ costs}$$

From the application of the two strategies we have obtained the *risk mitigated* (see risk mitigation in Table IV) and the *solution costs* (see direct costs in Table IV). To determine the third unknown, the *risk exposure*, Sonnenreich et al. [20] suggest to multiply the expected likelihood and expected severity of security incidents — in our case non-payments. As it is very difficult to determine a single number for the expected likelihood and the expected severity [21], we adopt the concept of Value at Risk (VaR). In its more general form, VaR measures the potential loss in value of a risky asset over a defined period of time for a given confidence interval. To calculate the VaR for our two different strategies we first need the aggregated loss distribution which at the same time requires determining the loss frequency and severity distributions. The frequency and severity of the non-payments (per week) are captured in the probability density histograms as displayed in Figure 5. For the loss frequency a normal distribution with a mean of 165 and standard deviation of 40 was fitted on the data. The loss severity was fitted with a gamma distribution with a shape of 2.5 and a rate of 0.1 (i.e. scale of $1/0.1 = 10$). The two distributions that were fitted are displayed in red, their mean, or expected, values are indicated with a green line.

To obtain the aggregated loss probability distribution function, we need to compound the frequency and severity probability distribution functions. We used a Monte Carlo simulation to estimate it by iterating $1,000,000$ times. Figure 5 shows the obtained aggregated loss distribution. The red line represents the normal distribution that was fitted on the data, with a mean of $4,100$ and standard deviation of $1,000$. The green line

[2]Assuming one FTE costs $ 150,000 on a yearly basis

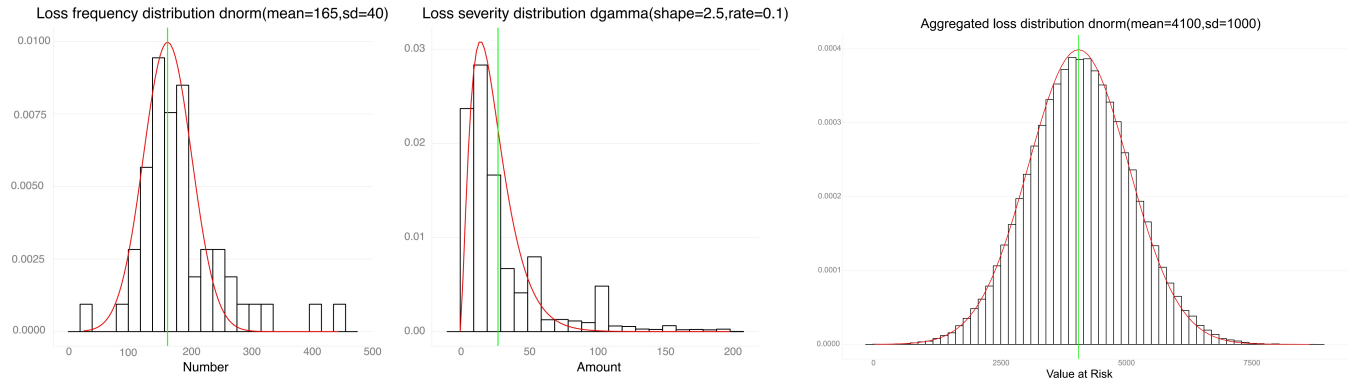

Figure 5. Loss frequency and loss severity distributions and aggregated loss distributions – segmented by week

represents the VaR of the distribution at a confidence interval of 50%. Moving the line to the left decreases the confidence interval of the VaR, moving the line to the right increases the interval.

When comparing the $ROSI$ curves, as visualized in Figure 6, we can observe that at a confidence interval of 50% of the VaR, the $ROSI$ value for the non-payment recovery process is positive while the $ROSI$ value for the random forest is around minus one. This implies that for each euro invested in the non-payment recovery process, more than one euro revenue is made, while investments in the random forest would result in a loss. No matter which confidence interval of the VaR is considered, the non-payment recovery process outperforms the random forest. Only at the far tails — i.e. at a very low or very high confidence — the ROSI values converge.

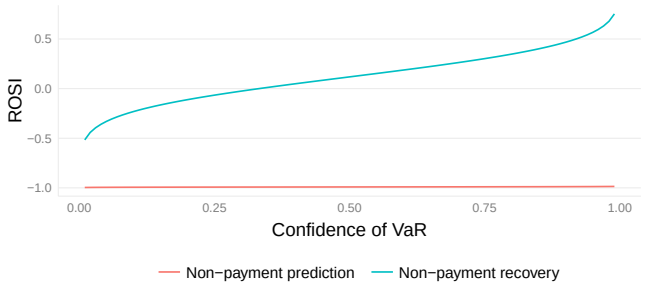

Figure 6. Strategy evaluation using the ROSI

V. DISCUSSION

Our assessment of the proposed risk mitigation strategies has to acknowledge the limitation that the evaluation has been conducted in the context of the TPP network under study, over a certain population of merchants and in a certain time frame. Although there is no reason to believe that the strategies will not perform similarly outside the DACH-region, this remains a topic for additional research. Besides the proposed mitigation strategies, we see opportunities for continued research into (1) optimizing the two proposed strategies, (2) designing new strategies and (3) combining preventive and reactive strategies for the development of a continuous risk management process.

For the continuous risk management process we would suggest to make use of the outcome of the non-payment recovery process to provide additional attributes for the non-payment prediction (random forest classifier), as visualized in Figure 7. As presented, we were able to capture the funds for 76% of all non-payment volume with the non-payment recovery process. We could argue that the consumers linked to these transactions are friendly fraudsters or no fraudsters at all. Then what about the remaining 24%? Are these transactions linked to the true fraudsters?

The feedback gathered from the non-payment recovery process might be beneficial to decrease the misclassification error of the random forest classifier, as the classifier can be trained using a better ground truth. It has the potential to decrease its direct costs (i.e. the misclassification cost linked to the false positives) and improve its risk mitigation (i.e. the classifier's accuracy) as a result. And as genuine consumers will be less hindered by the risk process, it is not unimaginable that they become more loyal shoppers, increasing benefits even further. We believe that this approach is not only beneficial for risk management in the TPP network, but can also enhance risk management in the card network.

Also, we see opportunities for future research outside

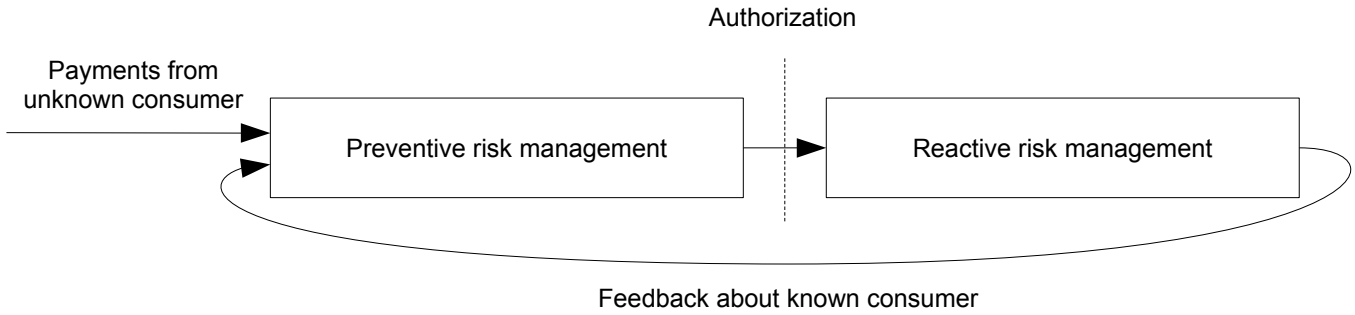

Figure 7. Combining preventive and reactive strategies for the development of a continuous risk management process

the scope of our own research. For example, what would happen if phishing would occur on the connection between the consumer and the TPP? Or what would happen if the connection between the TPP and the issuer would get compromised?

VI. CONCLUSION

Over the years, various initiatives have been launched to provide an alternative to the card network. One of the latest efforts is the introduction of PSDII within the European Union, requiring banks to open op their services to TPP networks. Although TPP networks are intended to realize a more integrated and efficient European payment market, they do suffer from the occurrence of non-payments, which share characteristics with chargebacks in the card network.

Non-payments occur when authorized transactions do not get settled. We identified that non-payments are more likely to occur outside business hours, at gaming and gambling related merchants, at payments initiated from mobile devices and at payments initiated from specific countries. Additionally, non-payments are concentrated on a small subset of issuers. Although this indicates that there are possibilities to fundamentally improve the functioning of the TPP network, the stakeholder who suffers the financial impact of the non-payments, the merchant, has little influence on realizing these improvements.

In our research we have proposed and evaluated two risk management strategies to mitigate the impact of non-payments. The strategies are intended to be deployed at the level of the traditional Payment Service Provider (PSP). The first strategy encompasses the deployment of a random forest classifier in order to estimate the likelihood that a transaction will end up in a non-payment before it occurred. The second strategy encompasses a non-payment recovery process in which the consumer is asked to pay his due amount when a non-payment occurred. By evaluating the effectiveness of the strategies using the Return on Security Investment Model ($ROSI$) and the Value at Risk (VaR) to quantify the risk exposure of the non-payments, we discovered that the reactive strategy is more cost effective than the preventive strategy encompassing the deployment of the random forest classifier. This implies that, although non-payments can be fraud related, it is at the moment not cost effective to prevent this fraud.

We believe that combining the two risk management strategies into a continuous risk management process can enhance the effectiveness of the risk process significantly. By leveraging the results of the non-payment recovery process, we are enabled to differentiate fraudulent from non-fraudulent non-payments, creating a better ground truth for the deployment of the random forest classifier. The better ground truth has the potential to decrease the cost of mis-classification and increase the classifier's accuracy. Because of the analogies between fraud within the TPP network and friendly fraud in the card network, we believe that this approach can also be beneficial to combat friendly fraud in the card network.

ACKNOWLEDGMENTS

Our research would not have been possible without the access to transaction data from the TPP network. We would like to thank PSP Adyen [22] for providing us with this data. Besides, we would like to thank everyone who contributed to our work, in particular Ross Anderson, for sharing their thoughts and providing valuable input during the research process.

REFERENCES

[1] L. M. Ausubel, "The failure of competition in the credit card market," *The American Economic Review*, pp. 50–81, 1991.

[2] D. S. Evans, "Economic aspects of bitcoin and other decentralized public-ledger currency platforms," *University of Chicago Coase-Sandor Institute for Law & Economics Research Paper*, no. 685, 2014.

[3] R. Anderson, "Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age," *Consumer Payment Innovation in the Connected Age*, pp. 99–120, 2012.

[4] European Commission, "European Parliament adopts European Commission proposal to create safer and more innovative European payments," http://europa.eu/rapid/press-release_IP-15-5792_en.htm, 2015.

[5] "Trustly Group AB," https://trustly.com.

[6] "Sofort GmbH," https://www.sofort.com.

[7] "CurrentC," https://www.currentc.com.

[8] "POLi Payments Pty Ltd," https://www.polipayments.com.

[9] R. P. DeGennaro, "Credit card processing: a look inside the black box," *Economic Review*, vol. 91, no. 1, pp. 27–42, 2006.

[10] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. Van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *The economics of information security and privacy*. Springer, 2013, pp. 265–300.

[11] CyberSource, "2013 Online Fraud Report: Online Payment Fraud Trends, Merchant Practices, and Benchmarks," http://www.cybersource.com/content/dam/cybersource/CyberSource_2013_Online_Fraud_Report.pdf, 2013.

[12] Office of the Federal Register (U.S.), *Code of Federal Regulations, Title 26, Internal Revenue, PT. 40-49, Revised as of April 1, 2011*. U.S. Government Printing Office, 2011.

[13] European Payment Council, "SEPA Credit Transfer (SCT)," http://www.europeanpaymentscouncil.eu/index.cfm/sepa-credit-transfer/sepa-credit-transfer-sct/.

[14] European Commission, "Commission Staff Working Document Impact Assessment," eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013SC0288.

[15] C. M. Kahn and W. Roberds, "Credit and identity theft," *Journal of Monetary Economics*, vol. 55, no. 2, pp. 251–264, 2008.

[16] International Monetary Fund, "Germany: Technical Note on the Banking Sector Structure," *Technical Report 11*, 2011.

[17] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical science*, pp. 235–249, 2002.

[18] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.

[19] European Payment Council, "SEPA Direct Debit (SDD)," http://www.europeanpaymentscouncil.eu/index.cfm/sepa-direct-debit/sepa-direct-debit-core-scheme-sdd-core/.

[20] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (ROSI)-a practical quantitative model," *Journal of Research and practice in Information Technology*, vol. 38, no. 1, pp. 45–56, 2006.

[21] R. Böhme and T. Nowey, "Economic security metrics," in *Dependability metrics*. Springer, 2008, pp. 176–187.

[22] "Adyen BV," https://www.adyen.com.