

Article

A New Card-Linked Loyalty Program: Estimated and Anticipated Benefits for Payment Transaction Parties

Albert Sitek  and Zbigniew Kotulski * 

Institute of Telecommunications of WUT, 00-665 Warsaw, Poland; albert.sitek@gmail.com

* Correspondence: z.kotulski@tele.pw.edu.pl

Received: 20 October 2020; Accepted: 14 November 2020; Published: 19 November 2020



Abstract: Electronic card payments are getting more and more popular, mainly because of their simplicity, convenience, processing time and high level of security. The fact that a single payment card is issued for a particular cardholder makes it possible to link a card to various services. In this paper, we investigated a usage of a payment card in the loyalty program that incorporates our Contextual Risk Management System (CRMS) to assure a novel intangible reward: Shorter transaction processing time. In the beginning, we emphasize the importance of soft benefits in modern loyalty programs and recall the risk management algorithms and the reputation system that has been used in the CRMS. Then, using an extensive dataset of 2.5 million payment transaction traces (collected within a year from 68 terminals) we estimate potential benefits for merchants and cardholders and try to predict an effect of this system for the future. We also discuss the impact of this system on the real and user-perceived security level.

Keywords: card-linked loyalty; contextual security; risk management; transaction security; payment card

1. Introduction

A loyalty program (LP) can be defined as “an integrated and interactive system of marketing actions that aim to make customers more loyal by developing a personalized relationship with them” [1]. LPs are a powerful marketing tool with plenty of advantages. According to recent statistics [2,3], 70% of customers are likely to recommend brands with good LPs, 43% of them spend more money at brands they are loyal to and LP members spend between 12 and 18% more per year than non-LP members. The same reports show that it costs five times more to acquire a new customer than it does to retain a returning one. Moreover, lowering the customer churn rate by 5% can increase the organization’s profitability by 25 to 125%. Importance of LPs has made them a “must-have” strategy for companies. Hence, it is no surprise that most retailers have introduced loyalty programs to remain competitive [4].

The heart and soul of a loyalty program are its benefits. They are usually divided into following groups [5,6]:

1. Hard (tangible) benefits: financial incentives like discounts, free hotel stays, vouchers (coupons, see [7]), tickets,
2. Soft (intangible) rewards: non-financial like preferential treatment, special events, an elevated sense of status, services, entertainment, priority check-in, and so on.

The loyalty program will only be successful if the right combination of benefits is chosen [5]. There are a lot of papers in the literature that discussed an issue of rewards in loyalty programs (e.g., [5,6,8–12]) and their findings are not unambiguous. For instance, an author of [6] claims the underlying effects of reward types on preferences and intended store loyalty differ depending on

the level of consumers' personal involvement. In the case of high personal involvement, intangible rewards and compatibility with the store's image, increase LP preference and loyalty. Additionally, the time required to obtain the reward (immediate/delayed) has no impact. In the case of low personal involvement, tangible and immediate rewards increase LP preference and loyalty. Compatibility with the store image does not matter. On the other hand, an author of [5] claims that no loyalty program should rely on discounts or other price breaks to create loyalty because "customer loyalty cannot be bought but must be earned". Furthermore, according to Walker [13], "by the year 2020 customer experience will overtake price and product as the key brand differentiator". Consequently, the key benefits should be non-financial and based on special treatment, communication, service and so on. What is more, traditional financially driven loyalty schemes can become a financial liability for businesses [14]. Moreover, in some countries, intangible rewards can be enforced by the law. Until recently, German law forbade selling the same product to different customers at different prices, e.g., depending on whether or not they were members of LP. That is why German marketers were forced to develop programs that created loyalty without financial incentives [5].

As shown above, intangible rewards are essential parts of a good loyalty program. Moreover, such a program should be beneficial for both parties of the transaction. That was our main motivation to propose a new non-financial incentive for loyal customers: shorter transaction processing time when a payment card is used [15]. In our previous paper, we presented a Contextual Risk Management System (CRMS) that is able to dynamically decide whether the cardholder verification is necessary during the certain transaction, or not. The decision is being made based on the historical transaction of the cardholder and other contextual factors like transaction amount, length of the queue, the content of the basket, the actual level of various security threats, and so on. The whole system is also able to maintain the level of acceptable risk. Its operation was simulated using productive data: more than 1 million of transaction traces collected from 68 payment terminals located in 18 shops, within 6 months. In this paper, we enhance our previous work and present simulation results of the CRMS using an extended dataset of productive transactions, containing almost 2.5 million records collected within one year. What is more, using the data collected from the terminals, we try to quantitatively estimate the increase of merchants' income due to application of the CRMS in a newly proposed loyalty program. This is so-called Card-Linked Loyalty Program: A solution that uses a payment card as a unique identifier in the loyalty program.

The rest part of this paper is organized as follows. Section 2 presents an evolution of loyalty programs from trading stamps towards modern solutions, including Card-Linked Loyalty Programs. We give an overview of goals and benefits of the programs. Especially we emphasize using payment card-based solutions and their advantages over other loyalty systems. Section 3 briefly recalls the CRMS: its architecture, used algorithms and main properties. It also compares the system applied in our studies with possible alternative solutions known from the literature. Section 4 gives a presentation of the dataset used in our experiments: where and how it has been gathered and how the data is protected to satisfy legal constraints. This Section contains results of simulations of the CRMS based on the extended dataset. Section 5 gives the main result of our analysis. It shows an estimation of anticipated benefits from the usage of the CRMS, to quantitatively express profits of application of our Card-Linked Loyalty Program in a really existing retail network. The final Section 6 concludes the paper and maps out future work on the CRMS and related loyalty systems.

2. An Evolution Towards Card-Linked Loyalty Programs

First reward programs started to exist around 1890 in the form of trading stamps: small paper coupons that were given to customers by merchants. They did not have any value itself, but a customer (after saving a certain quantity) could exchange them for other goods or services. At first, they were given to the customers who paid in cash, and not credit. After some time, merchants found that it is more profitable to give trading stamps to all customers. This form of a reward program gained huge popularity in the 1910s and 1920s when they spread across gas stations and supermarkets [16].

The most popular brand of trading stamps in the United States was “S&H Green Stamps”. It assumed that customers were given redeemable stamps called Green Stamps, based on how much they bought. This program, at the start of 1960, boasted that it printed three times more stamps than the number of postage stamps printed by the U. S. Post Office [17].

In the 1970s, trading stamps became less common, because serious inflation forced merchants to cut costs and discontinue such programs. Their role has been taken by reward programs offered by groceries, credit card companies and so on. Afterward, in 1981 American Airlines has developed its own reward program called Advantage Program, with miles as a currency. Since then, the design of reward program has changed drastically all over the world [18].

An author of [19] divided Loyalty Programs into 4 types:

1. Type I, where members take an additional discount at register,
2. Type II, where members take 1 free when they buy n units,
3. Type III, where members receive rebates or points based on cumulative purchase,
4. Type IV, where members receive targeted offers and mailings.

An essential point in the evolution of reward programs is that how the way of collecting points and redeeming rewards have changed. As mentioned above, first reward programs were based on a collection of some dedicated stamps or punching punch cards (Type I and II). In such a program a customer could be completely anonymous. Such an approach is simple, but from marketing and data mining point of view is not acceptable. That is why modern loyalty programs are account-based (Types III and IV) so that it is required that the customer will consciously join the program, by giving some of his/her personal data and accepting terms and conditions. In such a system the current state of the customer’s account is kept in a central database. So, the only issue is how a unique identifier of the customer’s account can be transferred to the Point-of-Sale system during the check-out process. This is changing in line with the development of technology. Starting from a magstripe card, through cards with barcode or QR code printed on it, ending with the utilization of smartphones, which can pass the identification data through NFC interface (like [20]), or display barcodes from various physical cards (like Stocard [21]). The recent research also presents how to use Blockchain for Loyalty Program [22,23]

There is also an emerging trend observed on the market to use a payment card as a unique identifier in the loyalty program. Such a technique is called Card-Linked Loyalty [24] and an example transaction flow can be as follows ([15]): During the payment transaction, a Point-of-Sale (POS) terminal reads the card number and verifies on the dedicated server if there are some discounts/promotions to be proposed to the customer. If yes, the customer can decide whether he wants to redeem an offered reward or not. Also, some bonus points can be added automatically after the transaction to the customer’s account.

Such an approach has many advantages:

1. It does not interrupt a payment process; Loyalty should be a part of the payment process and should not interrupt it [24],
2. It will work with payment card emulated via a smartphone through the NFC interface,
3. It does not need to enroll manually or online: sign up to the Loyalty Program during your payment,
4. It does not require to download dedicated applications, carry another plastic card or print off rewards or coupons (rewards can be redeemed during the payment process).

This technique is a subject of many U.S. Patents (e.g., [25–32]), but it has been firstly presented in the book [33], even before electronic card payment gained such a popularity. The author in this book emphasized the role of additional data that can be gathered from the smart card during the payment process in order to enable real-time marketing. He introduced the Transaction Richness Quotient that is a measurement tool rigorously quantifying the added value a particular payment method provides in real time at the moment of purchase. He also claimed that customer loyalty can be built through three complementary objectives [33]:

- Reward attribution; the ability to attribute rewards to the customer immediately, such as discounts or free items,
- Customer knowledge generation; the ability to generate useful knowledge about the customer and to make it instantly available at the payment terminal,
- Relationship building; the ability to establish a long-term relationship that is not necessarily based on financial rewards, but rather on soft benefits like preferential treatment.

Those objectives can be achieved by well-designed Card-Linked Loyalty Program. As described in Section 1, the solution described in this paper can be used in such LPs in order to assure soft benefit, which is the shorter transaction processing time.

The primary goal of a loyalty program is to establish a relationship with the customers that turn them into long term loyalty customers [18]. There are also other main goals of the loyalty program (see Figure 1):

- Win a new customer. This can be done in two ways [18]. Firstly, satisfied LP members increase their word of mouth advertising. Secondly, the value of the LP benefits themselves is so attractive that non-customers join the loyalty program. These new members will eventually try the product and will continue using it after a satisfactory initial experience.
- Build a strong database. A correctly designed loyalty program allows building a valuable database containing socio-demographic data together with information on purchase behavior (purchase frequency, brand usage) and preference data. This information is normally very difficult to obtain and used in a professional way can be a strategic weapon,
- Support other company departments. The database created in the scope of the previous point can assist other departments such as R&D, product marketing, or market research,
- Create communication opportunities. It allows for creating direct and personalized communication to the customer.

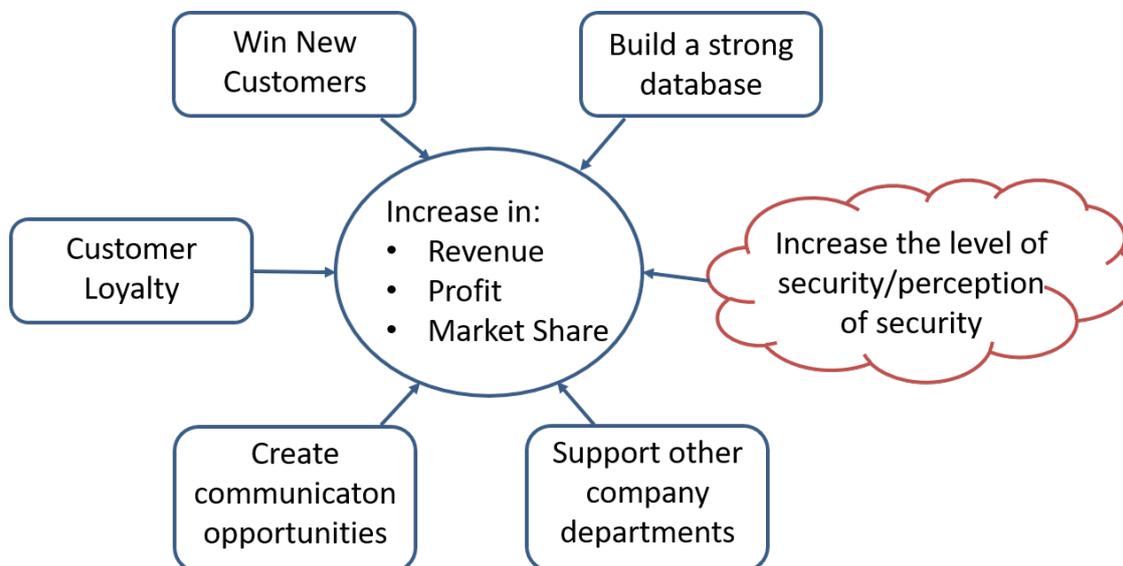


Figure 1. Main Goals of Customer Loyalty Programs, based on [5].

There is also an additional factor that can be treated as a goal of loyalty program: increase the level of security/perception of security. Nowadays, the cybersecurity is a field of knowledge extensively studied from different points of view, e.g., as development and implementation of new security countermeasures and security management schemes [34], as socioeconomic studies regarding the customer reactions following a major data breach [35], and as a range of technical and sociotechnical security controls applied from inside and outside of firms to detect threats, vulnerabilities and frauds [36]. In our approach an increase of transactions' cybersecurity is an indirect impact on

consumers' loyalty. In the era of various cyber-threats, the customer must feel safe in order to allow him to create a personal relationship with the seller. It is especially crucial in the e-commerce market because consumers' attitudes and beliefs about security have significant effects on the intention to purchase online. This is possible because customers no longer interact with a salesperson and must rely on electronic payment methods, which increases their perceived risk [37]. A lack of perceived security is a major reason why many potential consumers do not shop online because of common perceptions of risks involved in transmitting sensitive data, such as credit card numbers, across the Internet. Consumers, who provide personal information during transactions, assume the risk of having this information compromised [37].

3. Contextual Risk Management System for Card-Present Payment Transactions

In this section, we will familiarize the reader with the subject of contextual risk management in card-present (CP) payment transactions and present our solution called Contextual Risk Management System (CRMS).

A key motivation to investigate this issue is the fact that currently each card-present payment transaction is processed with constant parameters and rules (for instance, a request for a PIN entry when the transaction amount exceeded certain limit). Such an approach is simple, but not effective from multiple viewpoints. Not each payment transaction is related to the same level of risk. There is also a common perception that usability and security are competing goals ([38,39]), so it would be valuable to create the solution that will allow improving the usability of card-present payment transactions and will not destroy the security.

The security of modern card-present payment transaction is usually assured by the usage of two-factor authentication that utilizes the following components [40]:

1. What you have—a payment card that cannot be cloned (in case of modern chip cards),
2. What you know—a secret PIN code.

The fact that there is no possibility to clone chip cards causes that card-present payment transactions are only prone to the usage of lost or stolen cards. The analysis created by National Bank of Poland [41] presents the level of fraudulent transactions based on data gathered from Issuers (Banks) and Acquirers. It shows that:

- The number of transactions made with lost or stolen cards accounts for approximately 13% of all fraudulent transactions recorded by Issuers,
- According to acquirers, the number of fraudulent transaction accounts for 0.001% of all processed transactions.

As one can see, the probability that the given transaction is performed using a lost or stolen card is really low. Consequently, the main idea behind the contextual risk management in payment transaction is that it is possible to occasionally resign from some security mechanisms (e.g., PIN verification) when the level of risk related to the current transaction is below a certain limit.

The issue of context, contextual security and risk management are very popular in modern IT solutions. The important Gartner's report [42] has predicted contextual security solutions with adaptiveness a perspective approach to information security solutions in general. Now there are a lot of papers, norms and patents regarding those topics. For example, the standard [43] depicting information security risk management techniques is now fundamental in the area of information security management. It is supported by the standard of [44] defining external and internal context in details.

The issue of the contextual risk management in CP payment transaction has been firstly addressed by us in [45], where we proposed a new Cardholder Verification Method: One-time PIN. It assumed that each transaction was authorized online and the decision whether a PIN verification was necessary or not, should be made by the Issuer based on various contextual factors (like merchant's location,

time of the transaction, cardholder's reputation, the actual level of various security threats, etc.). In the case of a positive decision, encrypted PIN (or One-time PIN) was sent back to the terminal and a payment application verified if the encrypted PIN entered by the cardholder was the same as the one received from the Issuer. The mentioned paper showed that the research area of contextual risk management in payment transactions can bring a lot of benefits for various actors involved in a payment process.

Another approach has been proposed in [46], where we described the solution that allows to control payment transaction flow and decide whether the transaction should be authorized online or offline. The decision-making algorithm used in the solution utilizes, among other contextual factors, the value of cardholder's reputation calculated using a dedicated reputation system. Unfortunately, the mentioned system is not capable to detect all suspicious behaviors because it is not able to consider all possible transaction flows.

In order to improve and extend the previous solution, in the paper [47] we proposed a new Cardholder's Reputation System. It is able to cover all possible transaction flows and it assumes that each transaction flow has a constant rating assigned to it. After the transaction performed with a certain flow, a cardholder receives a proper rating. To gauge the cardholder's reputation before the forthcoming transaction, the system calculates a weighted average of ratings from last N transactions.

An interesting patent has been proposed by Tomasofsky et al. [48]. They classified the reputation into 4 values: Excellent, Good, Neutral and Negative. Furthermore, they connected these values with transaction limits. For example, in case of Neutral reputation there is a transaction limit equal to 5, Transaction Spending Limit equal to \$100, Daily Spending Limit equal to \$200 and Weekly Spending Limit equal to \$500.

All above-mentioned papers described various modifications and improvements to be used in the present card payment ecosystem. However, they were tested using synthetic datasets (prepared based on experts' knowledge), because of the scarcity of production data. There are a lot of papers that describe transaction traces. For example, the authors of the report [49] describe Transaction Context, Product Price and Demography, while the papers [50,51] depict Product Type. However, all these papers describe online transactions; to the Authors' best knowledge there is no paper that describes traces from the terminal. It was the main motivation for our further research described in the paper [52]. We proposed there a new approach to collect and analyze transaction traces gathered directly from a payment terminal. What is more, we have made an experiment in a production payment system, where we collected and analyzed more than 1 million transaction traces gathered from 68 payment devices located in 18 shops, within 6 months.

Based on our previous findings described above, in the paper [15] we proposed a complete solution called Contextual Risk Management System (CRMS). In the rest part of this section, we will briefly demystify key functionalities of the system and highlight used algorithms and methods.

At first, we will recall the key requirements that we had taken before we designed the system. We assumed that:

1. The system is responsible for making the dynamic decision whether the cardholder verification should be performed during the certain transaction or not,
2. It must be able to use some contextual factors in the decision-making process,
3. It must maintain the level of risk caused by the usage of the system,
4. The solution must be able to work with transactions performed using the contact and contactless payment cards,
5. The whole solution must operate on tokenized card data ([53]). Thanks to that it would not be a subject of Payment Card Industry Data Security Standard (PCI DSS, [54]) and requirements caused by General Data Protection Regulation (GDPR, [55]) are less strict because tokens are treated as pseudonymized personal data.

A high-level architecture of the system can be found in Figure 2. The transaction flow that involves usage of the CRMS looks as follows:

1. Payment terminal reads card’s data, tokenizes it and sends a request containing transaction amount and card token to the CRMS,
2. CRMS runs the decision-making algorithm and decides whether the cardholder verification step should be performed or not,
3. CRMS sends the response to the terminal, and the transaction is processed according to the system’s decision.

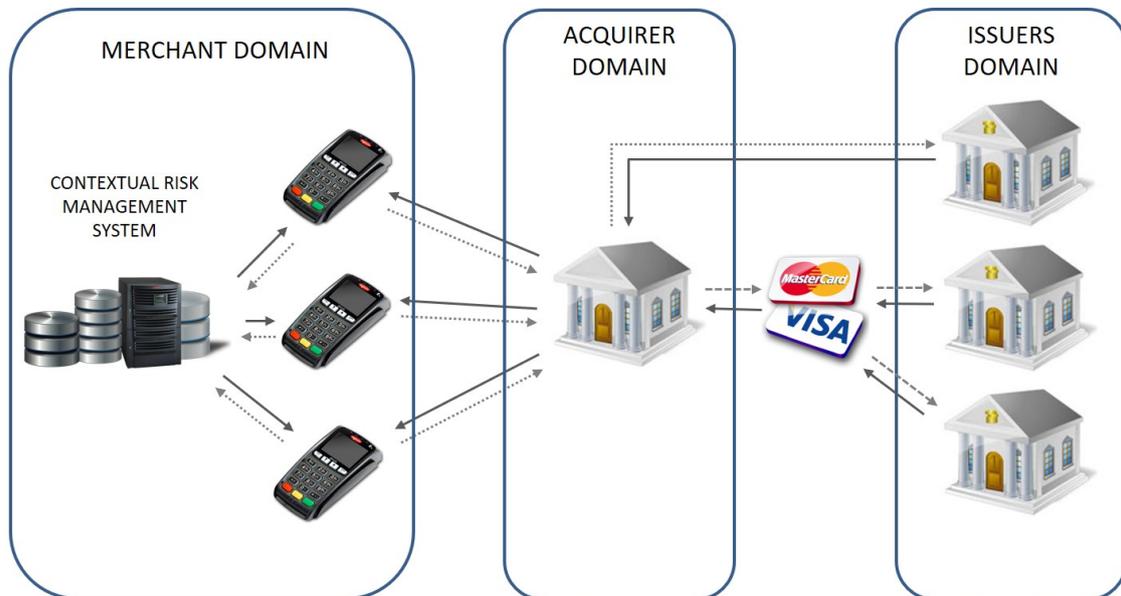


Figure 2. High-level Contextual Risk Management System architecture, based on [15].

The decision-making process looks as follows (see [15]):

$$\begin{cases} Risk_{curr} \leq Risk_{max} \Rightarrow \text{without Cardholder Verification} \\ Risk_{curr} > Risk_{max} \Rightarrow \text{with Cardholder Verification} \end{cases} \quad (1)$$

where $Risk_{max}$ denotes the maximum risk accepted by the merchant for a given transaction, and $Risk_{curr}$ is the level of the risk connected to the current transaction.

The value of $Risk_{max}$ can be dynamically adjusted taking into account some contextual factors like the content of the basket, the length of the queue, the actual level of various security threats, etc.

Generally speaking, the risk associated with a usage of the proposed system can be calculated as follows:

$$Risk_{curr} = a_{curr} * p, \quad (2)$$

where a denotes an amount of the current transaction, p is the probability that the current transaction will become fraudulent.

On the other hand, in order to take the Cardholder’s Reputation into account, following extension can be proposed:

$$Risk_{curr} = a_{curr} * p * f(R), \quad (3)$$

where $f(R)$ denotes an impact of Cardholder’s Reputation on theoretical risk. One can easily spot that the calculated $Risk_{curr}$ denotes the maximum theoretical loss per each transaction. $f(R)$ function should fulfill the following requirements:

- Should approach infinity for $R \rightarrow R_{min}$,
- Should have its minimum value for $R = R_{max}$.

It is worth noticing that the shape of $f(R)$ function has an impact on a few important facts:

- For which R , $f(R) = 1$: it means for what reputation, the calculated risk is equal to the estimated one?
- What is $f(R_{max})$: e.g., if $f(R_{max}) = 1/2$, it means that maximal reputation causes that calculated risk is half of the estimated one?

Assuming that the reputation $R \in \langle 0, R_{max} \rangle$, a good example of the function f that fulfills above-mentioned requirements, can be as below and in the Figure 3:

$$f(R) = \begin{cases} \infty & \text{if } R = 0 \\ \frac{a}{b \cdot R} & \text{if } R \in (0, R_{max}) \end{cases} \quad (4)$$

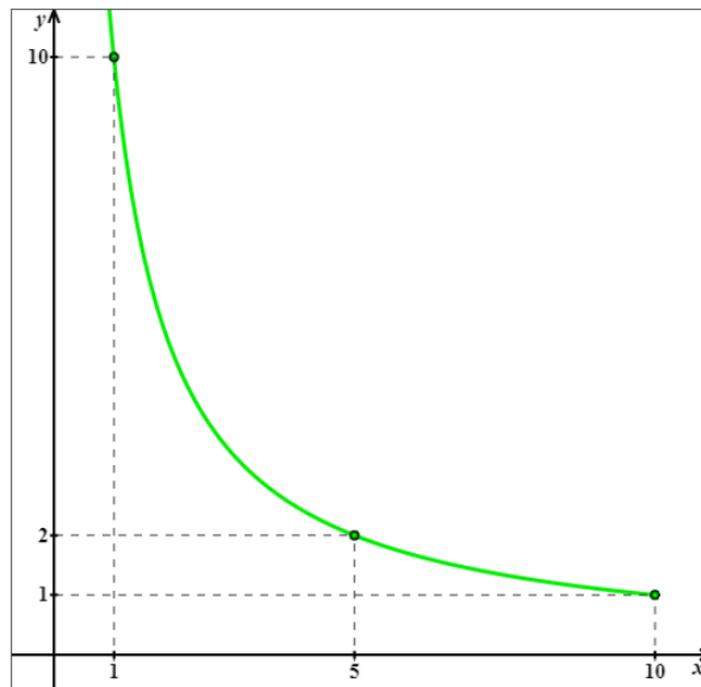


Figure 3. An example of the $f(R)$ function, where $R_{max} = 10$, $a = 10$ and $b = 1$.

3.1. Fraud Probability

There are a few types of Card Frauds: cloned card (skimming), usage of lost or stolen card or stolen card data to perform eCommerce transaction. Basically, presented CRMS is only vulnerable to the transactions made with the lost or stolen card, because it operates only with EMV compliant smartcards (these cards are not prone to cloning), and because it works only for card present transactions.

Next, we will try to evaluate the fraud probability by the example of the Polish market. The report created by the National Bank of Poland [41] presents the level of fraudulent transactions based on data gathered from Issuers (Banks) and Acquirers. It presents that:

- An average amount of fraudulent transaction is 830.40 PLN,
- The number of transactions made with lost or stolen cards accounts for approximately 13% of all fraudulent transactions recorded by Issuers,
- According to Acquirers, the number of fraudulent transaction accounts for 0.001% of all processed transactions.

It is worth mentioning that we forecast the presented system to operate (on Polish market) for transactions with the maximum amount of 200 PLN. Based on that, we estimate fraud probability at the level of 0.000001. This is the value used for further simulations. For more details please refer to [15].

3.2. Cardholder's Reputation System

The cardholder's reputation R is the reputation value calculated using a formula described in [47]. It is calculated as a weighted average based on flows of past N transactions performed by a given cardholder. Weights are calculated using following formula:

$$w_{Rni} = \frac{1}{2} e^{-\frac{t_n - t_i}{\tau_{RT} * AvgT}} * \operatorname{erfc}\left(\frac{(n - i - 1) * 2}{x_d} + x_m\right), \quad (5)$$

where n is the index of current transaction, i is the index of i -th transaction, t_i is time of i -th transaction, t_n is time of current transaction, $AvgT$ is the average distance between transactions, τ_{RT} is the reputation system parameter (the decay factor), erfc is the Complementary Error Function, x_d is the reputation system parameter (a dispersion parameter of the erfc function), x_m is the reputation system parameter (a concentration parameter of the erfc function) [56]).

Calculated Reputation is between R_{min} and R_{max} values:

$$R_n = \begin{cases} R_{min} & \text{if } \bar{R}_{n-i} < R_{min} \\ \bar{R}_{n-i} & \text{if } \bar{R}_{n-i} \in \langle R_{min}, R_{max} \rangle, \text{ where } i \in \langle 1, N \rangle. \\ R_{max} & \text{if } \bar{R}_{n-i} > R_{max} \end{cases} \quad (6)$$

This formula was proposed based on the series of tests and simulations. For more details please refer to [47].

4. The Experiment

As described in Section 1, in order to perform an accurate estimation of profits that can be taken from the usage of the CRMS in a Card-Linked LP, at first we redid simulations described in the paper [15] using the extended dataset of productive transaction traces, originally described in the paper [52]. The mentioned dataset is around two times bigger than previously used. It contains 2,463,203 transactions' traces made using 293,795 unique payment cards, collected within 1 year in 18 shops belonging to one of the retail chains. All those shops are located in the Northwest region of Poland, near the border with Germany. The location of the shops causes that there is a part of the traces that illustrates occasional buyers, but the rest part of the traces is sufficient to build the reputation system. Moreover, buyers did not know if their payment is recorded—that is why the results is not intentionally abused. The technique used to fulfill security requirements is called pseudonymization; that is why a couple of records can be linked to the one person, but the person is not known.

The aim of the experiment was to simulate “what will happen if the proposed CRMS was deployed in the given retail chain”. To do so, we implemented all the above-mentioned mechanisms and algorithms, and simulated operation of the CRMS in production. To do so, we implemented dedicated Python's scripts with following libraries:

- NumPy (fundamental package for scientific computing [57]),
- pandas (the library providing high-performance, easy-to-use data structures, and data analysis tools [58]),
- Matplotlib (plotting library [59]).

An example of such a function can be seen in Figure 4. We wrote our scripts in IPython [60] (the system for interactive scientific computing). As an IDE (Integrated Development Environment) we used Jupyter [61]. After that, we took the transaction history of each card token and checked which historical transaction would have been processed without cardholder verification. After that, we performed various analyses on the received results, including:

- What was the number of transactions selected to be processed without cardholder verification?
- What was the summary amount of the transactions above?

- What was the number of cardholders with almost one transaction promoted by the CRMS?
- What was the total gain in time caused by the usage of the system?
- What was the maximum loss caused by the usage of the system versus maximum loss when no cardholder's reputation was taken into account?
- What was the maximum cost for the merchant to gain one minute of time, to promote one transaction, and to promote one cardholder?

```

def int_calc_curr_r(trans, date):
    avg_t = 0
    reputation = 0

    for i in range(-1, -past_trans-1, -1):
        avg_t = avg_t + (date - trans.iloc[i].date).days
    avg_t = avg_t/past_trans

    for i in range(-1, -past_trans-1, -1):
        value = trans.iloc[i].rate

        time_diff = (date - trans.iloc[i].date).days
        exp = 1/2
        if avg_t != 0:
            exp = (1/2)*np.exp(-(time_diff / (t_rt*avg_t)) )
        erfc = special.erfc( ( ( -(i+1) * 2) / xd) + xm)
        reputation += value*exp*erfc
    return reputation

```

Figure 4. An implementation of the function that calculates Cardholder's Reputation.

We performed 16 simulations for values of $Risk_{max}$ (expressed in the Polish currency: PLN—"Polish zloty") from the range between 0.005 PLN and 0.02 PLN, which correspond to the maximal transaction amount without a cardholder verification from 50 PLN up to 200 PLN. In the rest part of this section, we present the results of our simulations.

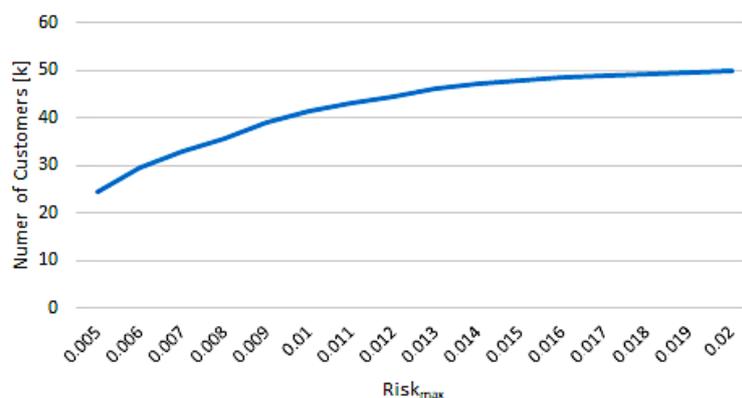


Figure 5. Customers with at least 1 transaction selected.

Figure 5 presents the number of customers with at least 1 transaction selected by the CRMS for processing without PIN verification, during a simulated period of time. This number varies from 24,493 to 49,933, which is from 8.33% to 17% of all recorded card tokens. On the other hand, the number of all selected transactions can be found in Figure 6. It shows that this number varies from 127,313 up to 305,691, which is from 5.17% to 12.41% of all transactions. It is worthy to note that the total amount of selected transaction varies from 3,247,951 PLN to 15,822,076 PLN, see Figure 7. It is also worthy to mention that we received much better result than during our first simulation described in the paper [52] (6.19% to 12.49% and 4.58% to 10%, respectively), but still they are relatively low. In our opinion, such a situation could happen because the transaction traces have been collected near the Polish-German border, where there are a lot of tourists visiting this area and buying goods and services occasionally. Moreover, nowadays the majority of cardholders are using more than one payment card.

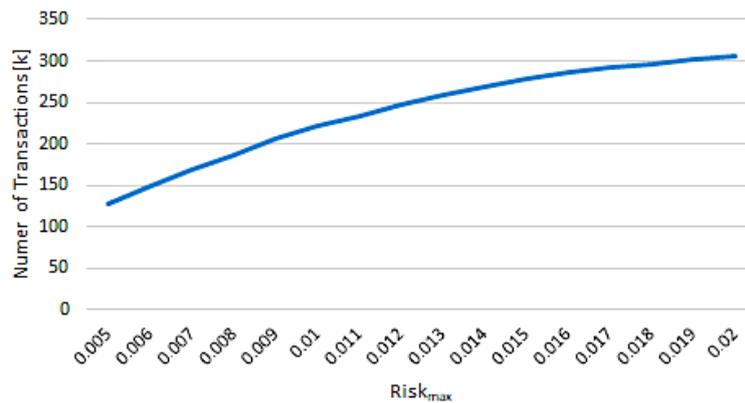


Figure 6. Number of selected transactions.

Figure 8 shows the time gained because of the usage of the CRMS. It has been measured as a difference between the summary amount of transaction processing time originally observed in the productive transaction traces, and the results of simulations (when the CRMS was enabled). This time varies from 9353 up to 24,029 min, which stands for 155.9 to 400.5 h. This result is almost 3 times bigger than previously (58.5 up to 135.5 h). We must admit that this time is very impressive, considering that we analyzed transaction traces from 18 stores collected within one year. Next, in Figure 9 one can see the collation between theoretical maximal loss caused by the usage of the CRMS and maximal loss calculated from the results of our simulation. In other words, it shows an impact of cardholder’s reputation and $f(R)$ function on maximal losses. Such a perspective is valuable during setting the CRMS’s parameters. As expected, new results show that maximal losses increase proportionally to the gain of time. Finally, Figure 10 shows the maximal cost that must be paid for rewarding a single cardholder (to select at least one transaction made by a certain cardholder), selection of one transaction or for gaining one minute of processing time. Such a piece of information is crucial for the merchant during the selection of accepted risk for the CRMS.

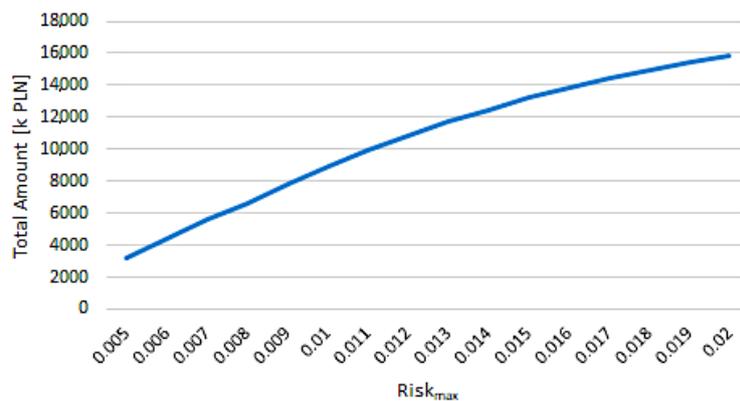


Figure 7. Total amount of all selected transactions.

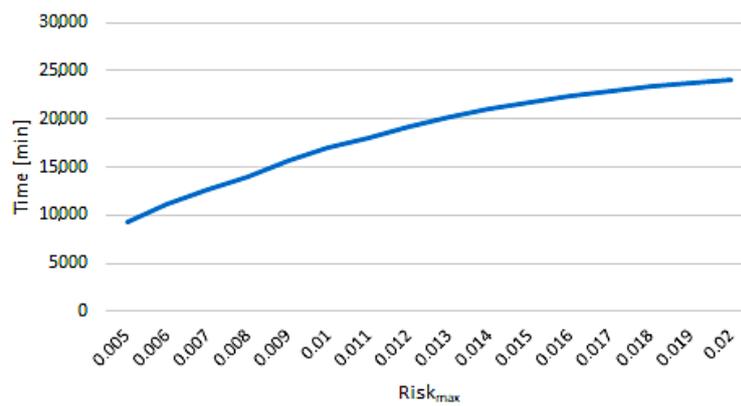


Figure 8. Time gained caused by the usage of the system.

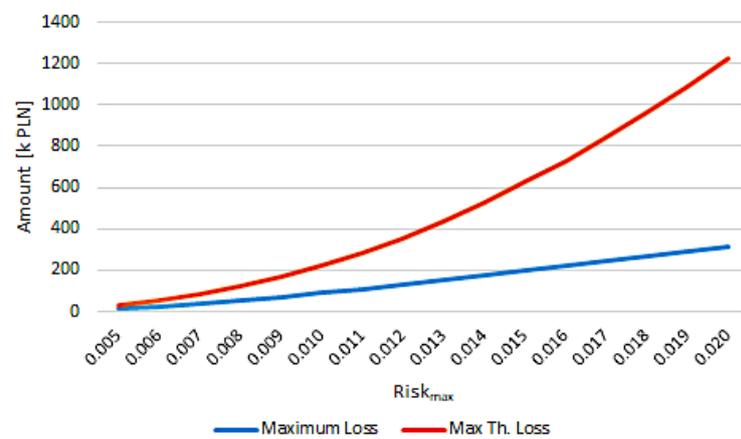


Figure 9. Maximal losses.

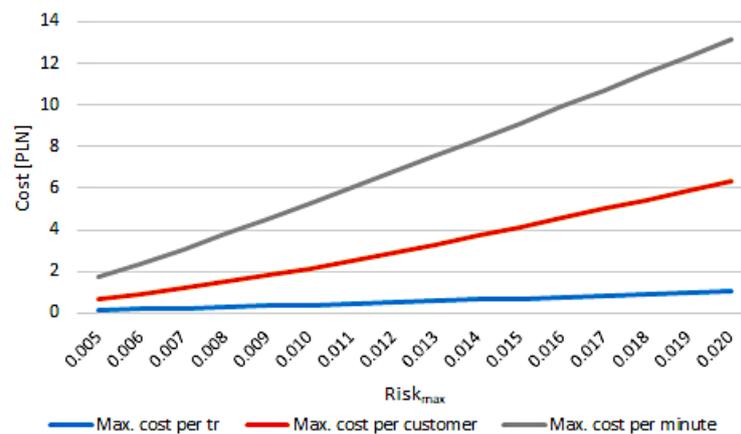


Figure 10. Max cost per one promoted cardholder, selected transaction and gained minute.

5. Profits Estimation

There is no doubt that the key benefit of the usage of the CRMS is a reduction of average processing time during a payment transaction, keeping the risk on the accepted level. In order to begin an estimation of real profits, we changed simulation scripts described in the previous section, so that it will be possible to illustrate how the selection of the payment transaction will be changing in time. Additionally, we focused on one representative value of $Risk_{max}$ equal to 0.01. Results can be observed in Figures 11 and 12. Based on them we can admit that:

1. The time required for the CRMS to achieve a destined number of selected transactions to be processed without cardholder verification is about 3–4 months,
2. During the first month since the CRMS started, the profits are negligibly low.



Figure 11. A number of selected transactions per month, for $Risk_{max} = 0.01$.

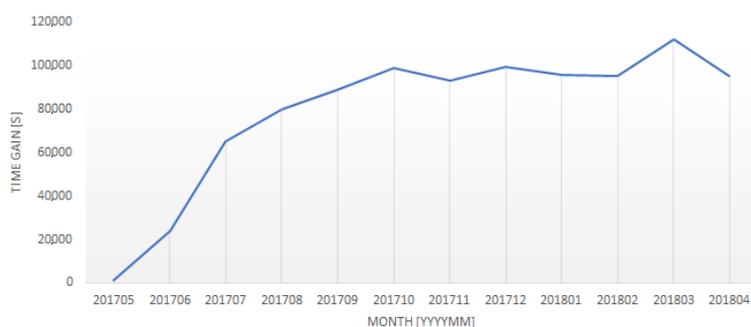


Figure 12. A simulated gain of the time per month, in seconds, for $Risk_{max} = 0.01$.

In order to estimate the real gain of time, we took the most pessimistic assumption that the start of the Loyalty Program did not have an impact on the number of transactions and on their amounts. Additionally, according to the information published by ZenCard Loyalty Program (a Card-Linked Loyalty Program from Poland, see [62]), around 60% of customers that pay with a payment card join to their service. We can safely assume that the majority of customers which transactions have been selected during our simulation would have joined such a loyalty program. In the view of above, for the purpose of our estimates, we have adopted that 80% selected transactions had been performed by the clients belonging to the loyalty program. Additionally, assuming that the gain of time for a single transaction is constant and that there was the same number of selected transactions for each payment cards, an estimation of gain of time for $Risk_{max}$ equal to 0.01 can be observed in Figure 13.

From our results, we can see that after the CRMS reaches its full performance, the gain of time for the analyzed 18 shops will be around 21.2 h per month. This value can be further recalculated to direct profits like savings from overtime, but this strongly depends on a given shop.

There are also some additional benefits for a merchant from having a loyalty program, for example, an increase in the value of the transaction, the number of clients, etc. However, it is not possible to estimate such benefits because they strongly depend on other features of a loyalty program, for instance, whether it gives some tangible rewards like discounts, coupons, and so on.



Figure 13. An estimated gain of the time per month, in hours, for $Risk_{max} = 0.01$.

6. Conclusions

In this paper, we presented the estimation of the benefits for payment transaction parties that can be gained from the usage of Contextual Risk Management System in Card-Linked Loyalty Program. We did our estimation based on the results of the simulations performed using almost 2.5 million traces of productive payment transactions from Polish shops. Our findings have shown that the CRMS can bring significant benefits for both: merchants and cardholders, and it is a valuable source of intangible reward in the loyalty program: shorter transaction processing time. Of course, our model can be utilized in different countries, but similar tests have to be conducted there. The reputation calculation model proposed in our considerations is simple but sufficiently flexible to adapt its parameters to customers' shopping habits in different countries, including frequency, volume, contents of the basket, etc. So, the proposed Card-Linked Loyalty Program is quite universal and can be implemented in any national, cross-border or international retail network.

The crucial component of our loyalty system is the reputation system, the CRMS. The mode of action of the CRMS allows to occasionally skip the cardholder verification during the transaction processing. This fact makes the cardholder aware that the PIN verification is not only a technical activity, but it is a factor strictly related to the security of the transaction, depending on cardholder's reputation and his/her activity. The way how the CRMS works gives an impression of constant dialog between the system and the cardholder. He/she can be sure that the system will react appropriately to his/her behavior. If only the system allows skipping a cardholder verification during the first transaction (for the amount above cardholder verification limit), it will indicate to the cardholder a failure of the system. An evolution of the proposed solution could give a cardholder the opportunity to choose if he/she would like to redeem shorter transaction processing time or to continue building the reputation, saving it for the future transactions. Moreover, the CRMS is part of the modern trend of increasing the limits of payment transactions without authorization, especially after COVID-19 experience [63,64]. In our system, instead of checking the PIN for randomly chosen transactions below the increased fixed limit, we propose building the customer reputation. This solution allows maintaining a similar level of the transaction risk, and also builds a specific bond between the customer and the retail network.

Our model of Contextual Risk Management System in Card-Linked Loyalty Program has been proposed and tested for the card-based payment transactions. However, it can also be used for other e-commerce transaction whether 3D Secure should be used or not. It could be used for other security solutions for the payment systems, but such applications need additional studies to be practical applicable.

In our opinion, it would also be valuable to focus future research on various enhancements in simulation process (e.g., to collect traces also from Point-of-Sale (including the length of the queue, the content of the basket, and so on)). Such modifications would be suitable for extension of the model to an adaptive solution where the decision on how to authorize the transaction would depend not only on the customer's current reputation, but also on the degree of crowding the store. The system

would decide whether to expedite a transaction or build a customer reputation for future transactions. The preparation of a pilot implementation of the whole solution and interrogative survey among a group of cardholders, inquiring about an attitude to such a system, would also be worthwhile.

Author Contributions: Conceptualization, A.S. and Z.K.; methodology, Z.K.; software, A.S.; validation, A.S.; formal analysis, Z.K.; investigation, Z.K.; resources, A.S.; data curation, A.S.; writing—original draft preparation, A.S.; writing—review and editing, Z.K.; visualization, A.S.; supervision, Z.K.; project administration, A.S. Both authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: We would like to thank the management of the retail chain to allow us to carry out our experiments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Meyer-Waarden, L. The effects of loyalty programs on customer lifetime duration and share of wallet. *J. Retail.* **2007**, *83*, 223–236. [CrossRef]
2. Bond Brand Loyalty; Visa. The Loyalty Report 2018. Available online: <https://info.bondbrandloyalty.com/loyalty-report-2018> (accessed on 10 October 2020).
3. 13 Brand Loyalty Statistics You Need to Know to Keep Your Customers Coming Back. Available online: <https://www.fundera.com/resources/brand-loyalty-statistics> (accessed on 9 February 2019).
4. Theng So, J.; Danaher, T.; Gupta, S. What do customers get and give in return for loyalty program membership? *Aust. Mark. J.* **2015**, *23*, 196–206.
5. Butscher, S.A. *Customer Loyalty Programmes and Clubs*; Taylor & Francis: Abingdon, UK, 2017.
6. Meyer-Waarden, L. Effects of loyalty program rewards on store loyalty. *J. Retail. Consum. Serv.* **2015**, *24*, 22–32. [CrossRef]
7. Ferrer-Gomila, J.L.; Hinarejos, M.F.; Huguet-Rotger, L. A survey on electronic coupons. *Comput. Secur.* **2018**, *77*, 106–127. [CrossRef]
8. Xie, K.L.; Chen, C.C. Progress in Loyalty Program Research: Facts, Debates, and Future Research. *J. Hosp. Mark. Manag.* **2013**, *22*, 463–489. [CrossRef]
9. Uncles, M.D.; Dowling, G.; Hammond, K. Customer Loyalty and Customer Loyalty Programs. *J. Consum. Mark.* **2003**, *20*, 294–316. [CrossRef]
10. Dorotic, M.; Bijmolt, T.; Verhoef, P. Loyalty Programmes: Current Knowledge and Research Directions. *Int. J. Manag. Rev.* **2011**, *14*. [CrossRef]
11. McCall, M.; Voorhees, C. The Drivers of Loyalty Program Success. *Cornell Hosp. Q.* **2010**, *51*, 35–52. [CrossRef]
12. Keh, H.T.; Lee, Y.H. Do reward programs build loyalty for services?: The moderating effect of satisfaction on type and timing of rewards. *J. Retail.* **2006**, *82*, 127–136. [CrossRef]
13. Walker Information. *Customers 2020: A Progress Report*; Walker Information: Indianapolis, IN, USA, 2019.
14. The Deloitte Consumer Review Customer Loyalty: A Relationship, Not Just a Scheme. 2017. Available online: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-customer-loyalty.pdf> (accessed on 9 February 2019)
15. Sitek, A.; Kotulski, Z. On a New Intangible Reward for Card-Linked Loyalty Programs. In *Proceedings of the Advances in Soft and Hard Computing: 21th International Multi-Conference on Advanced Computer Systems, ACS 2018, Miedzyzdroje, Poland, 24–26 September 2018*; Advances in Intelligent Systems and Computing; Pejaś, J., El Fray, I., Hyla, T., Kacprzyk, J., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; Volume 889. [CrossRef]
16. Turner, M.A. *Credit Card Rewards: Context, History, and Value*; PERC Press: London, UK, 2012; Available online: <https://www.perc.net/wp-content/uploads/2013/12/WP-2-Layout.pdf> (accessed on 10 April 2019).
17. Larson, J.; McClellan, B.C.L. *Capturing Loyalty: How to Measure, Generate, and Profit from Highly Satisfied Customers*; Praeger: Westport, CT, USA, 2017.

18. Varma, A.J. Effectiveness of Customer Loyalty Programs a Study on Select Retailers in Bangalore and Mysore City. Ph.D. Thesis, University of Mysore, Mysore, India, 2015.
19. Berman, B. Developing an Effective Customer Loyalty Program. *Calif. Manag. Rev.* **2006**, *49*, 123–148. [[CrossRef](#)]
20. Smets, J.; Ergeerts, G.; Beyers, R.; Schrooyen, F.; Ceulemans, M.; Wante, L.; Renckens, K. An NFC-based Customer Loyalty System 2011. In Proceedings of the First International Conference on Resource, Services and User Mobility, Barcelona, Spain, 23–28 October 2011; Available online: <https://www.semanticscholar.org/paper/An-NFC-based-Customer-Loyalty-System-Smets-Ergeerts/df882ff5c00729881cd1c1234f987f9cd76f07c6> (accessed on 19 November 2020).
21. Stocard Homepage. Available online: <https://stocardapp.com/en/au> (accessed on 9 February 2019).
22. Antoniadis, I.; Kontsas, S.; Spinthiropoulos, K. Blockchain and Brand Loyalty Programs: A Short Review of Applications and Challenges. In Proceedings of the International Conference on Economic Sciences and Business Administration, Bucharest, Romania, 15–16 November 2019. [[CrossRef](#)]
23. Wang, L.; Luo, R.; Hua, Y. Exploring How Blockchain Impacts Loyalty Program Participation Behaviors: An Exploratory Case Study. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Grand Wailea, HI, USA, 8–11 January 2019. [[CrossRef](#)]
24. vPromos. How Does Card-Linking Loyalty Work? 2016. Available online: <https://www.vpromos.com/> (accessed on 26 February 2019).
25. Chien, E.; Sanchez, T.; Saunders, D.; Wiseman, J.; Balagopal, C.R.; Kinderknecht, A.; Parson, J.W.; Preston, R. System and Method for Using Loyalty Rewards as Currency. U.S. Patent 8,265,993 B2, 25 October 2012.
26. Hessburg, M.B.; Rappleyea, A.W.; Rodriguez, S.; Sanoff, J.; Silverstein, A.N. System and Method for Exchanging Loyalty Points for Acquisitions. U.S. Patent 7,686,218 B2, 9 November 2010.
27. Aloni, R.L.; Axelrod, B.T.; Bowman, J.L.; Funda, J.J.; Polon, J.S.; Tiku, S.V.; American Express Travel Related Services Co Inc. Loyalty Incentive Program Using Transaction Cards. U.S. Patent 9,665,880 B2, 30 August 2017.
28. Robison, S.K. Customer Loyalty Program. U.S. Patent 2003/0200141 A1, 10 October 2003.
29. Friday, G.; Leece, R.; Snyder, L.; Turnbull, A.; Pearce, G.; Madden, R.; Panayotopoulos, C.; Castle, A.; Bank of Nova Scotia ScotiaBank; InfiStar Corp; et al. Cardholder Loyalty Program with Rebate. U.S. Patent 2005/0240477 A1, 27 October 2005.
30. Trzcinski, J.R. Generic Universal Rewards Loyalty Card. U.S. Patent 2011/0238471 A1, 29 September 2011.
31. Fontana, A.J.; Onay, O.; Tabachnick, G.; Switchly Inc.; Topguest. Loyalty Program Systems and Methods. U.S. Patent 2012/0284108 A1, 8 November 2012.
32. Fordyce, E.W., III; Amaro, L.; Winters, M.E.; Griggs, A.W.; DiGioacchino, L.; Salmon, D.C.; Siegel, K.P.; Subramanian, K.; VonDerheide, J.A.; Visa USA Inc. Systems and Methods to Provide Loyalty Programs, WO Patent 2012/0284108 A1, 14 April 2011.
33. Haddad, A. *Using Smart Cards to Gain Market Share*; Gower: Swansea, UK, 2000.
34. Cabaj, K.; Domingos, D.; Kotulski, Z.; Respicio, A. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Comput. Secur.* **2018**, *75*. [[CrossRef](#)]
35. Goode, S.; Hoehle, H.; Venkatesh, V.; Brown, S. User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach. *MIS Q.* **2017**, *41*, 703–727. [[CrossRef](#)]
36. Goode, S.; Lacey, D. Detecting complex account fraud in the enterprise: The role of technical and non-technical controls. *Decis. Support Syst.* **2011**, *50*, 702–714. [[CrossRef](#)]
37. Chang, H.H.; Chen, S.W. Consumer perception of interface quality, security, and loyalty in electronic commerce. *Inf. Manag.* **2009**, *46*, 411–417. [[CrossRef](#)]
38. Sepczuk, M.; Kotulski, Z. A new risk-based authentication management model oriented on user's experience. *Comput. Secur.* **2018**, *73*, 17–33. [[CrossRef](#)]
39. Weir, C.S.; Douglas, G.; Carruthers, M.; Jack, M. User perceptions of security, convenience and usability for ebanking authentication tokens. *Comput. Secur.* **2009**, *28*, 47–62. [[CrossRef](#)]
40. Gunson, N.; Marshal, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Comput. Secur.* **2011**, *30*, 208–220. [[CrossRef](#)]
41. Department of Payment System, National Bank of Poland. *An Assessment of the Functioning of Polish Payment System in 1st q. 2017*; Department of Payment System, National Bank of Poland: Warsaw, Poland, 2017. (In Polish)

42. MacDonald, N. *The Future of Information Security Is Context Aware and Adaptive*; Gartner Research: Hong Kong, China, 2010.
43. IEC/FDIS 31010:2009 *Risk Management—Risk Assessment Techniques*; ISO: Geneva, Switzerland, 2009.
44. BS/ISO 31000:2018 *Risk Management—Guidelines*; ISO: Geneva, Switzerland, 2018.
45. Sitek, A. One-time code cardholder verification method in electronic funds transfer transactions. In *Annales UMCS ser. Informatica*; Universitatis Mariae Curie-Skłodowska: Lublin, Poland, 2014; Volume 14, pp. 46–59.
46. Sitek, A.; Kotulski, Z. Contextual management of off-line authorisation in contact EMV transactions. *Telecommun. Rev. Telecommun. News* **2015**, *88*, 953–959. (In Polish)
47. Sitek, A.; Kotulski, Z. Cardholder’s Reputation System for Contextual Risk Management in Payment Transactions. In *Proceedings of the Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, 28–30 August 2017*; Lecture Notes in Computer Science; Rak, J., Bay, J., Kottenko, I., Popyack, L., Skormin, V., Szczypiorski, K., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2017; Volume 10446, pp. 158–170. [[CrossRef](#)]
48. Tomasofofsky, C.P.; Hubbard, S.E.; Gerber, J.; Salazar, C.; Hafner, M.; Mastercard International Inc. Systems and Methods for Providing Risk Based Decisioning Service to the Merchants. U.S. Patent 10,614,452 B2, 7 April 2020.
49. Bounie, D.; Francois, A. Cash, Check or Bank Card? The Effects of Transaction Characteristics on the Use of Payment Instruments. In *Proceedings of the FMG & CASS Business School Conference (Workshop on Financial Regulation and Payment Systems), Milan, Italy, 6–10 May 2009*; SciTePress: Setúbal, Portugal, 2009; Available online: <https://www.semanticscholar.org/paper/Cash%2C-Check-or-Bank-Card-The-Effects-of-Transaction-Bounie-Fran%2C%27ois/b121c7b212ffb4097a2c3a3e994086662ae7bf7> (accessed on 10 October 2020).
50. Chiou, J.S.; Ting, C.C. Will you spend more money and time on internet shopping when the product and situation are right? *Comput. Hum. Behav.* **2011**, *27*, 203–208. [[CrossRef](#)]
51. Zhang, H.; Li, H. Factors affecting payment choices in online auctions: A study of eBay traders. *Decis. Support Syst.* **2006**, *42*, 1076–1088. [[CrossRef](#)]
52. Sitek, A.; Kotulski, Z. POS-originated transactions traces as a source of contextual information for Risk Management Systems in EFT transactions. *EURASIP J. Inf. Secur.* **2018**, *2018*, 5. [[CrossRef](#)]
53. Tokenization Taskforce, PCI Security Standards Council. PCI DSS Tokenization Guidelines, 2011. Available online: https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf (accessed on 18 November 2020).
54. PCI DSS Homepage. Available online: <https://www.pcisecuritystandards.org/> (accessed on 26 January 2019).
55. European Parliament. REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing DIRECTIVE 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union* **2016**. Available online: <https://www.europarl.europa.eu/portal/en> (accessed on 26 January 2019).
56. Kotulski, Z.; Szczepinski, W. *Error Analysis with Application in Engineering*; Springer: Dordrecht, The Netherlands, 2010.
57. Numpy Homepage. Available online: <https://numpy.org> (accessed on 26 January 2019).
58. Pandas Homepage. Available online: <https://pandas.pydata.org> (accessed on 26 January 2019).
59. Matplotlib Homepage. Available online: <https://matplotlib.org> (accessed on 26 January 2019).
60. Pérez, F.; Granger, B.E. IPython: A System for Interactive Scientific Computing. *Comput. Sci. Eng.* **2007**, *9*, 21–29. [[CrossRef](#)]
61. Jupyter IDE Homepage. Available online: <https://jupyter.org> (accessed on 26 January 2019).
62. ZenCard. Homepage. Available online: <https://www.finat.pl/narzedzia-marketingowe/> (accessed on 26 January 2019).

63. Fiserv's STAR to Increase PINless Transaction Approval Limits to USD 100. Available online: <https://thepaypers.com/digital-identity-security-online-fraud/fiservs-star-to-increase-pinless-transaction-approval-limits-to-usd-100--1242113> (accessed on 10 October 2020).
64. PIN-Less Payments Limit Goes Up as Coronavirus Countermeasure. Available online: <https://polandin.com/47285858/pinless-payments-limit-goes-up-as-coronavirus-countermeasure> (accessed on 10 October 2020).

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).