June 2020

Risk-appropriate Restrictions on Payment Options

Vishu Goyal

Ming Zhang

Vikas Sukla

Geoffrey Levine

Lin Shi

See next page for additional authors

Inventor(s)
Vishu Goyal, Ming Zhang, Vikas Sukla, Geoffrey Levine, Lin Shi, Padraig O'Mathuna, Andrei Harangus, Gargi M Keeling, and Monica Kuchinski

Risk-appropriate Restrictions on Payment Options

ABSTRACT

An online merchant faces at least two types of risks: a financial risk, e.g., the risk that a customer may not pay for goods and services purchased, and a platform risk, e.g., the risk that a customer may abuse the platform or violate the terms of service. This disclosure describes techniques that integrate models of financial and platform risk to generate a consolidated risk profile for a customer. The risk assessment model is proactively applied at the time of customer sign-up to identify high-risk customers. Payment option restrictions are applied to customers deemed to be high risk, e.g., restrictions on direct debit payments, threshold payments (up-front credit for purchases), the use of credit cards, etc. The techniques enable smooth sign-up and ease of use for low-risk customers and mitigate risk created by high-risk customers.

KEYWORDS

- Risk modeling
- Financial risk
- Platform risk
- Direct-debit abuse
- Payment options
- Online merchant

BACKGROUND

Online merchants offer a variety of payment options, e.g., credit card, direct debit, digital wallet, mobile banking applications, etc. Some of these payment options have a greater degree of susceptibility to abuse. For example, in some locations, a customer can easily cancel a direct debit payment for up to eight weeks after the payment is made and the procedure for the online merchant to recover purchased goods or services from the customer is time consuming. Such a practice by customers who make direct-debit payments with the intention of later canceling them is known as direct-debit abuse.

An online merchant faces at least two types of risks: a financial risk, e.g., the risk that a customer may not pay for goods and services purchased, and a platform risk, e.g., the risk that a customer may abuse the platform or violate the terms of service. Both types of risk are generally assessed using machine-learning (ML) models. For example, the financial risk of signing up a new customer is assessed by feeding to an ML model with relevant customer information.

DESCRIPTION

This disclosure describes techniques that integrate models of financial and platform risk to generate a consolidated risk profile of a customer. The risk assessment model is proactively applied at the time of customer sign-up to identify high-risk customers. Payment-option restrictions can be applied to customers deemed to be high risk, e.g., restrictions on direct-debit payments, threshold payments (up-front credit for purchases), the use of credit cards, etc. The techniques enable smooth sign-up and ease of use for low-risk customers and mitigate risk created by high-risk customers.

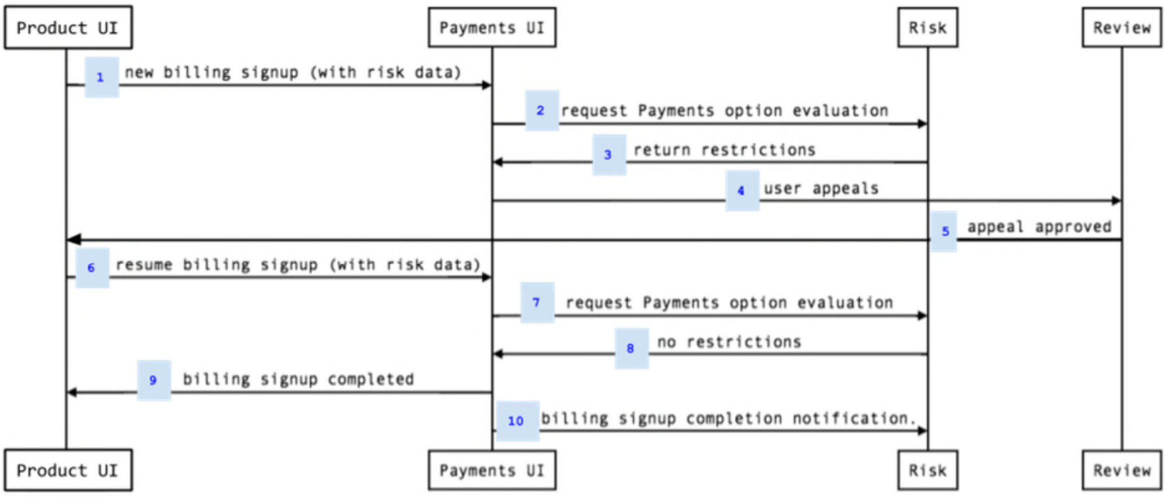

Product UI
Payments UI
Risk
Review
1 new billing signup (with risk data)
2 request Payments option evaluation
3 return restrictions
4 user appeals
5 appeal approved
6 resume billing signup (with risk data)
7 request Payments option evaluation
8 no restrictions
9 billing signup completed
10 billing signup completion notification.
Product UI
Payments UI
Risk
Review

Fig. 1: Risk-appropriate restrictions on payment options

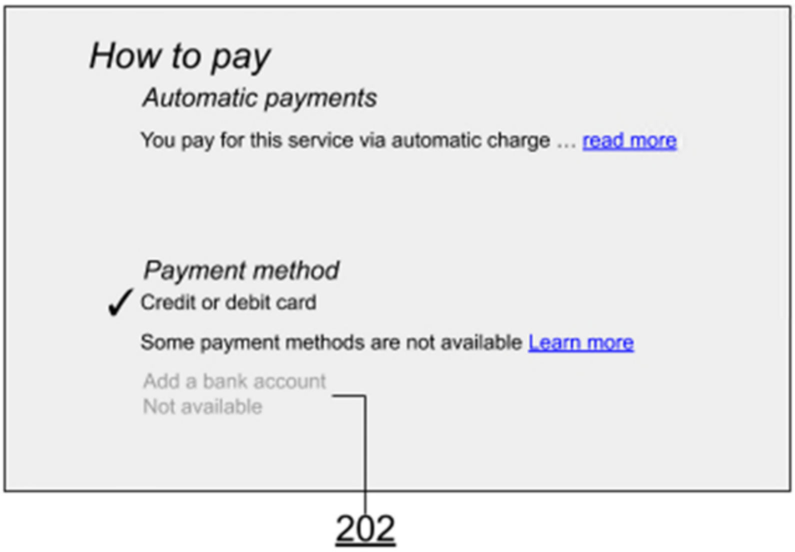
Fig. 1 illustrates the assessment of risk and the imposition of risk-appropriate restrictions on payment options, per the techniques of this disclosure. The example of Fig. 1 is applicable generally to online vendors, merchants, and other entities that face both platform as well as financial risk. An online merchant has internal processes or teams identified as follows.

- **Product UI:** Product user interface
- **Risk:** Includes assessment of the risk of platform abuse and assessment of the risk of financial abuse
- **Payments:** payments user interface, e.g., payments processing
- **Review:** operations review

Upon receipt of a request from a new customer to sign up for an account, the following events occur:

1. Product UI requests sign-up for a new billing account from Payments UI.
2. Payments UI requests a payments options evaluation from Risk.
3. Risk returns payment-option restrictions to Payments UI.

4. The new customer may appeal the payment-option restrictions to Review.
5. Operations Review may approve (or reject) the appeal, and communicate the results of the appeal. If the appeal is rejected, then the payment-option restrictions remain.
6. If the appeal is approved, Product UI resumes billing signup.
7. Payments UI requests a payments option evaluation from Risk .
8. Risk responds with reduced (or no) restrictions.
9. Payments UI completes the billing account sign-up requested by Product UI.
10. Payments UI notifies Risk of the completed billing account sign-up.



How to pay

Automatic payments

You pay for this service via automatic charge … read more

Payment method

✓ Credit or debit card

Some payment methods are not available Learn more

Add a bank account
Not available

Fig. 2: User interface indicating restrictions on certain payment methods

Fig. 2 illustrates an example user interface provided to a new customer. The user interface is based on the techniques of joint platform and financial risk modeling disclosed herein. Although some forms of payment, e.g., credit or debit card, are seen as enabled, other forms of payment, e.g., bank account direct debit, have been disallowed (202). A new customer can click on “learn more” to file an appeal.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user’s social network, social actions or activities, profession, a user’s preferences, or a user’s current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user’s identity may be treated so that no personally identifiable information can be determined for the user, or a user’s geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

An online merchant faces at least two types of risks: a financial risk, e.g., the risk that a customer may not pay for goods and services purchased, and a platform risk, e.g., the risk that a customer may abuse the platform or violate the terms of service. This disclosure describes techniques that integrate models of financial and platform risk to generate a consolidated risk profile for a customer. The risk assessment model is proactively applied at the time of customer sign-up to identify high-risk customers. Payment option restrictions are applied to customers deemed to be high risk, e.g., restrictions on direct debit payments, threshold payments (up-front credit for purchases), the use of credit cards, etc. The techniques enable smooth sign-up and ease of use for low-risk customers and mitigate risk created by high-risk customers.