Gumenyuk A., PhD., assoc. prof.,
Tkachuk A., PhD.,
Yanchuk V., PhD., assoc. prof.,
Zhytomyr State Technological University

SAVING CREDIT CARD DATA IN YOUR CUSTOMER PROFILE AT ECOMMERCE SOLUTIONS

These days we tend to take decisions quick and the main aspect making our life easier – is to make the operation as quick as possible. We purchase products and services online and we create more and more orders at different services. The biggest value of such turnover is to have optimal solutions that enables saving client sensitive data and lets to make the purchase in one click.

Fig 1. Example of the wallet use. The image is taken form the web-site https://pay.kyivstar.ua/mk/en/

A very bright example is the service of Portmone, which is wide-spread in Ukraine and former NIS Countries. The service is comprising all the best practices keeping cards on the wallet.

In fact, e-Wallet is an electronic card which is used for transactions to be made online via computer or a mobile device operating with debit or credit card data. In fact, the e-Wallet is linked with the individuals' bank account to make payments via credit card data.

For e-wallet it is sufficient to have a pre-paid account in which a user can store personal expenses (money) for any future online transaction. An E-wallet is protected with a password. Using an E-wallet you can make payments for groceries online purchases, and flight tickets, among others.

Each e-Wallet has mainly two components: the software and information. The software component stores personal information and provides security and encryption of the data. The information component is a database of details provided by the user which includes the name, shipping address, payment method, amount to be paid, credit or debit card details, etc.
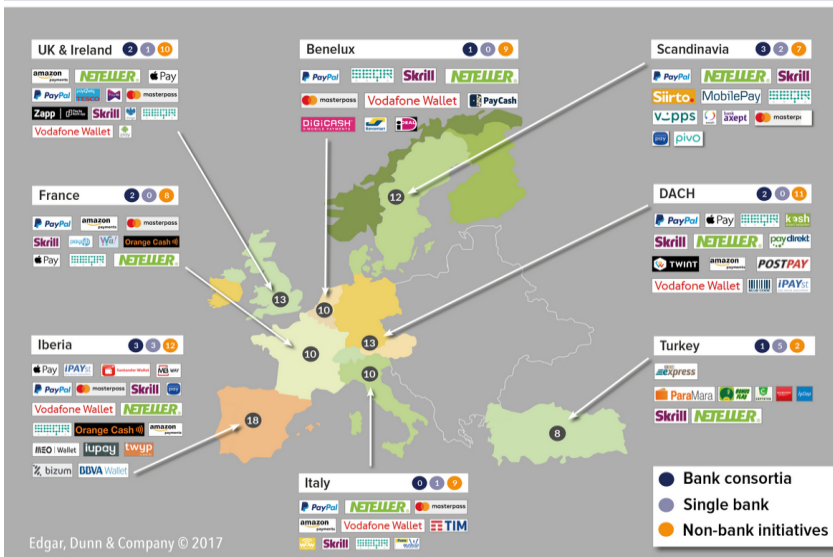
Fig 2. Wallets diversity in European market. Taken from [1]

However there are many vendors that mimic the functionality of e-Wallets and want to act without specific accounts, but want them to store this information inside the eCommerce platforms where they have variety of payment providers processing customer data.

Tokenization came to our life along with Pre-authorization services circulating in the world of goods and services.

In our recent publications [2-3] it has been described variety of mechanisms of making payments via ACH, CreditLine and CreditCard. CreditLine is renewed monthly with payments and it has a huge shift towards use of the Credit Card, especially with the mechanism of transaction expenses capturing, also so-called preauthorization. The below image indicates how pre-authorization happens in the world of services, represented by medical service.
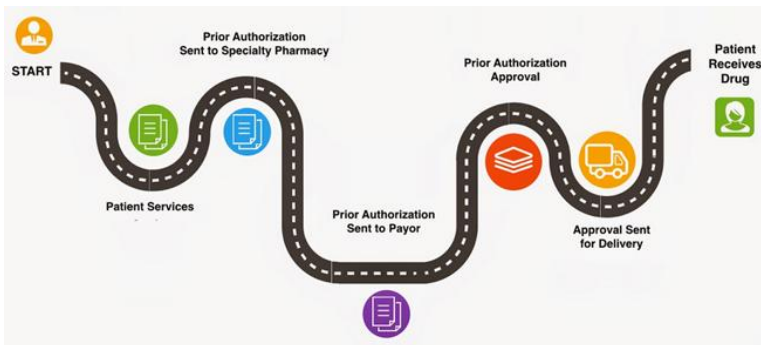

Fig. 3. Preauthorization in action. Transformed from [4]

Looking at the diagram from the fig. 3 we see how the process flows and the withdrawal is not happening, just reservation until the real customer is assured the parcel is coming to him. The money will not leave the bank account of the client. In the United States most of states has this as a local requirement and vendors are obliged to follow the regulation.

In the world of credit-card terminal usage happens pretty much the same for hotel services and healthcare. The below image demonstrates how the flow goes when the terminal is used. The process is nearly the same unless the verification of vendor and notification system works in a different manner. The general flow is standardized, that makes verification process easier and transparent.
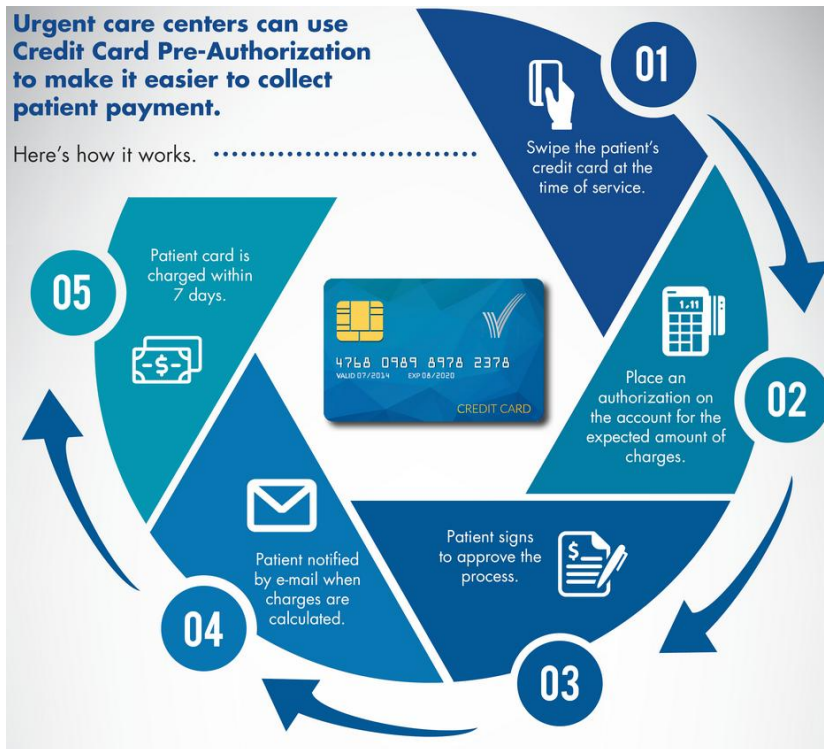
Fig. 4. Preauthorization with the card terminal [5]

Contemporary platforms are using OAUTH services, that opens great possibility to share the token across applications, that potentially influences the security circle of the payment method, where the customer may use the same token, which is not the part of this article, will be reviewed in further works. Let us concentrate how the consumer key is easily passed in the application.

To begin the process, you need to pass the Consumer Key and Consumer Secret to the service to acquire a Request Token. You will get given this when you register your application with the site [6].

```
// Acquire Request Token
OAuth["consumer_key"] = ConsumerKey;
OAuth["consumer_secret"] = ConsumerSecret;
OAuthResponse requestToken =
    OAuth.AcquireRequestToken("http://api.soundcloud.com/oauth/request_token", "POST");
```

Now that we have the request token, we need to prompt the user to grant us permission. If you are using a desktop application like I am in this example, use System.Diagnostics.Process to open a new browser window with the URL.

```
// Start the browser to get our access token
var url = "http://soundcloud.com/oauth/authorize?oauth_token=" + OAuth["token"];
System.Diagnostics.Process.Start(url);
```

As we have seen the solution with Tokenization is rather common and easy to implement and opens great perspective for the online marketing activities, however that requires proper implementation to keep it secure and respect the Global Data Processing Regulation (GDPR) and PCI compliance, which is not always the case.

References:

1. https://www.mobeyforum.org/european-digital-wallet-landscape/
2. Gumenyuk A., Yanchuk ACH and E-CHECK vs Credit Cards payment solutions: commission and security issues: Тези доповідей IX Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2018» (20–21 квітня 2018 р.). – Житомир : Вид. О. О. Євенок, 2018. – 296 с. С. 57-60.
3. Gumenyuk A., Yanchuk Payment solutions online using credit cards: online tracking vs threats and security risks Тези доповідей II Міжнародної науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення – 2017» (17–19 жовтня 2017 р.). – Житомир: Вид. О. О. Євенок, 2017. – 252 с. С: 17-18
4. https://www.drugchannels.net/2015/05/taking-specialty-prior-authorization.html
5. https://www.practicevelocity.com/how-use-credit-card-pre-authorization-urgent-care/
6. https://deanhume.com/a-simple-guide-to-using-oauth-with-c/