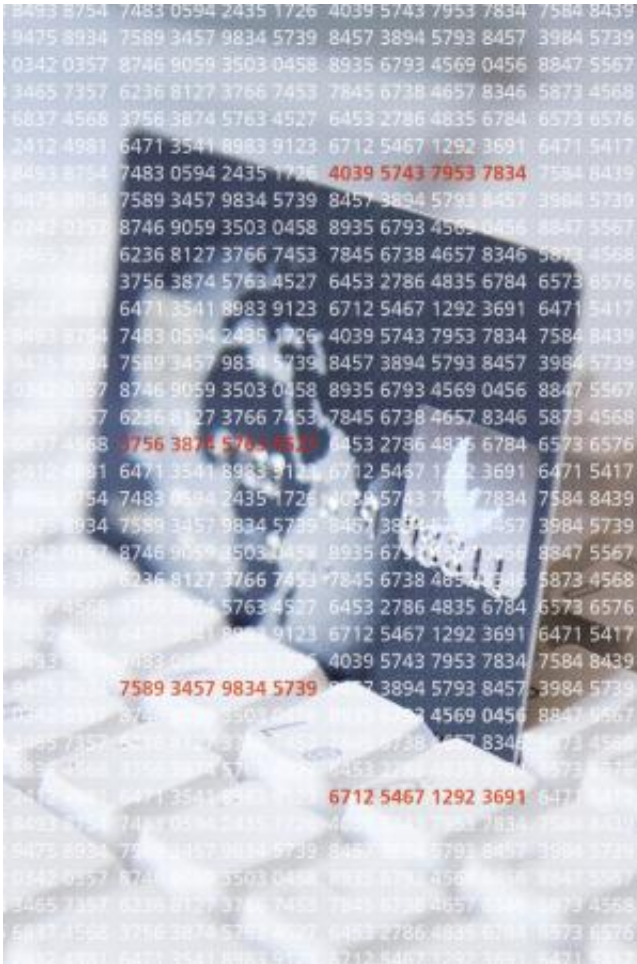


Credit card fraudsters quickly exposed

May 15 2013



With “MINTify rule” software, attempts to commit credit card fraud can quickly be exposed. Credit: Fraunhofer IAIS

Most people feel safe from fraudsters if their credit card is safely tucked away in their wallet. But they shouldn't: in most cases, thieves only need

card numbers and information. A new software can provide more effective protection against credit card theft.

A look at your account balance has just given you a shock: what's going on here? While you have spent the last few weeks in the office and definitely haven't travelled abroad, your account balance shows that you bought electronics in Turkey and ate out in France. In such situations, customers just have to call their banks to get their money back. But this often means that the banks lose the money.

How can credit cards be better protected? Exercising caution with your [wallet](#) and keeping the card in your hands when using it is no longer enough: a restaurant's card reading device can be infected with Trojans without the restaurant owner being aware of it. These Trojans then pass the customer's [credit card information](#) on to third parties. Customers are also at risk when they purchase something online. For this reason, banks have introduced if-then rules that stop purchases from other countries if a certain amount is exceeded. In such cases, the card [reading device](#)'s display shows a note indicating that the bank has refused to make the payment. Until now, bank employees have examined fraud cases manually and applied rules accordingly. But in recent years, cases of [credit card fraud](#) have exploded in number, and this approach has quickly reached its limits.

Rapid texting

The "MINTify rule" software now supports bank employees and helps them apply appropriate rules. The software was developed by researchers at the Fraunhofer Institute for [Intelligent Analysis](#) and [Information Systems](#) IAIS in Sankt Augustin, in cooperation with their partners at PAYMINT. "Our software analyzes recent transactions that are stored in the [credit card](#) company's database. Depending on the size of the company, there can be as many as one million data sets per

month," says Dr. Stefan Rüping, group manager at IAIS. "For these transactions, the software searches all possible rules and selects the ten to one hundred best options. The best thing about this program is that it finds the most suitable rules in 30 minutes to an hour." Over time, the researchers aim to make the system even faster, with the procedure lasting just a few minutes. Once this goal has been achieved, the software will also be attractive for companies trading in equity markets.

The banks must define a ratio between the levels of security they want for specific types of cards and consequently how many customers may then not be able to use their cards. The more fraudsters are stopped, the more real customers will face the problem of not being able to make a payment. In an ideal scenario, all fraudsters would be stopped and all customers would be served, but this is not feasible. A more realistic ratio would be "four [fraudsters](#) to one customer." Based on this aim, "MINTify rule" can initiate its analysis and select the best possible rules. "At some point it becomes clear whether or not a transaction was legal. The software can learn from this data," says Rüping. In addition, the rules that the security application finds are easy to understand. As a result, bank employees can either take the time to validate the rules or activate them directly.

The "MINTify rule" software is already being used at some banks as well as at a leading European payment processor, and provides protection for millions of credit cards. The software could also provide support in a number of other areas: for instance, it could help doctors at hospitals in the process of selecting medications.

Provided by Fraunhofer-Gesellschaft

Citation: Credit card fraudsters quickly exposed (2013, May 15) retrieved 23 April 2024 from <https://phys.org/news/2013-05-credit-card-fraudsters-quickly-exposed.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.