Foreword

Payment card fraud is a major challenge for business owners, payment card issuers, and transactional services companies, causing every year substantial and growing financial losses. According to the 2019 Nilson Report, card fraud losses worldwide have increased from 9.84 billion dollars in 2011 to 27.85 billion dollars in 2018, and are projected to reach more than 40 billion dollars in 2027 [rep19].

Detecting fraud patterns in payment card transactions is known to be a very difficult problem. With the ever-growing amount of data generated by payment card transactions, it has become impossible for a human analyst to detect fraudulent patterns in transaction datasets, often characterized by a large number of samples, many dimensions, and online updates. As a result, the design of payment card fraud detection techniques has increasingly focused in the last decade on approaches based on machine learning (ML) techniques, that automate the process of identifying fraudulent patterns from large volumes of data [CLBC+19, DP15, PP19, SSB18].

The integration of ML techniques in payment card fraud detection systems has greatly improved their ability to more efficiently detect frauds, and assist payment processing intermediaries in identifying illicit transactions. Though in recent years the number of fraudulent transactions kept on increasing, the percentage of losses due to fraud started to decrease in 2016, a reverse trend that is associated with the increasing adoption of ML solutions [rep19]. On top of helping saving money, implementing ML-based fraud detection systems is today becoming a must-do for institutions and companies to gain the trust of their customers.

A widely recognized and recurrent issue in this new field of ML for card fraud detection is the lack of reproducibility of most of the research work published on the topic [LJ20, PL18, PP19, ZAM+16]. On the one hand, there is a lack of availability of payment card transaction data, which cannot be publicly shared for confidentiality reasons. On the other hand, authors do not make enough efforts to provide their code and make their results reproducible.

This book aims at making a first step in the direction of reproducibility in the benchmarking of payment card fraud detection techniques. Due to the vast amount of published research in the domain, it was not possible to exhaustively review and implement all existing techniques. Rather, we chose to focus on some of the techniques that appeared to us as the most essential, based on our 10-year collaboration with our industrial partner Worldline.

Some of the techniques presented, such as those dealing with class imbalance or ensembles of models are widely acknowledged as being essential parts of the design of a credit card fraud detection system. We additionally cover less well-documented topics that we think deserve more attention. These include in particular design aspects of the modeling process, such as the choice of performance metrics and validation strategies, and promising preprocessing and learning strategies such as feature embeddings and neural networks in general.

While the book focuses on payment card fraud, we believe that most of the techniques and discussions presented in this book can be useful to other practitioners working on the wider topic of fraud detection.

With the reproducibility of experiments as a key driver for this book, the choice of a Jupyter Book format appeared better suited than a traditional printed book format. In particular, all the sections of this book that include code are Jupyter notebooks, which can be executed independently either on the reader's computer by cloning the book repository, or online using Google Colab or Binder. Additionnally, the open-source nature of the book - fully available on a public Github repository - allows readers to open discussions on the book content thanks to Github issues, or to propose amendments or improvements with pull requests.

License

The code in the notebooks is released under a GNU GPL v3.0 license. The prose and pictures are released under a CC BY-SA 4.0 license.

If you wish to cite this book, you may use the following:

```
@book{leborgne2022fraud,
title={Reproducible Machine Learning for Credit Card Fraud Detection - Practical Handbook},
author={Le Borgne, Yann-A{\"e}l and Siblini, Wissam and Lebichot, Bertrand and Bontempi, Gianluca},
url={https://github.com/Fraud-Detection-Handbook/fraud-detection-handbook},
year={2022},
publisher={Universit{\'e} Libre de Bruxelles}
}
```

Authors

- Yann-Aël Le Borgne (Contact author - yann-ael.le.borgne@ulb.be) - Machine Learning Group - Université Libre de Bruxelles, Belgium.
- Wissam Siblini - Machine Learning Research - Worldline Labs
- Bertrand Lebichot - Interdisciplinary Centre for Security, Reliability and Trust - Université du Luxembourg, Luxembourg
- Gianluca Bontempi - Machine Learning Group - Université Libre de Bruxelles, Belgium

Acknowledgments

This book is the result of ten years of collaboration between the Machine Learning Group, Université Libre de Bruxelles, Belgium and Worldline.

- ULB-MLG, Principal investigator: Gianluca Bontempi
- Worldline, R&D Manager: Frédéric Oblé

We wish to thank all the colleagues who worked on this topic during this collaboration: Olivier Caelen (ULB-MLG/Worldline), Fabrizio Carcillo (ULB-MLG), Guillaume Coter (Worldline), Andrea Dal Pozzolo (ULB-MLG), Jacopo De Stefani (ULB-MLG), Rémy Fabry (Worldline), Liyun He-Guelton (Worldline), Gian Marco Paldino (ULB-MLG), Théo Verhelst (ULB-MLG).

The collaboration was made possible thanks to Innoviris, the Brussels Region Institute for Research and Innovation, through a series of grants which started in 2012 and ended in 2021.

- 2018 to 2021. *DefeatFraud: Assessment and validation of deep feature engineering and learning solutions for fraud detection*. Innoviris Team Up Programme.
- 2015 to 2018. *BruFence: Scalable machine learning for automating defense system*. Innoviris Bridge Programme.
- 2012 to 2015. *Adaptive real-time machine learning for credit card fraud detection*. Innoviris Doctiris Programme.

Next
1. Book content and intended audience ›