SESSIONE PITCH 3

IT Architecture, Security & Governance

BankSealer – Il sistema di supporto semiautomatizzato alle decisioni per l'analisi delle frodi nell'Online Banking

Alvise Biffi, *Founder*, Secure Network

Claudio Caletti, *Founder*, Buildo

BANKSEALER

Catch financial frauds. The smart way.

BANKSEALER

ABOUT US

- Spin off
  - **Politecnico di Milano (strong academic background)**
    - Top engineering technical university in Italy
  - **Secure Network s.r.l. (top industry experience)**
    - Leading security firm in Italy
  - **buildo s.r.l.s. (software engineering expertise)**
    - Experts in delivering high quality software products

POLITECNICO
MILANO 1863

buildo

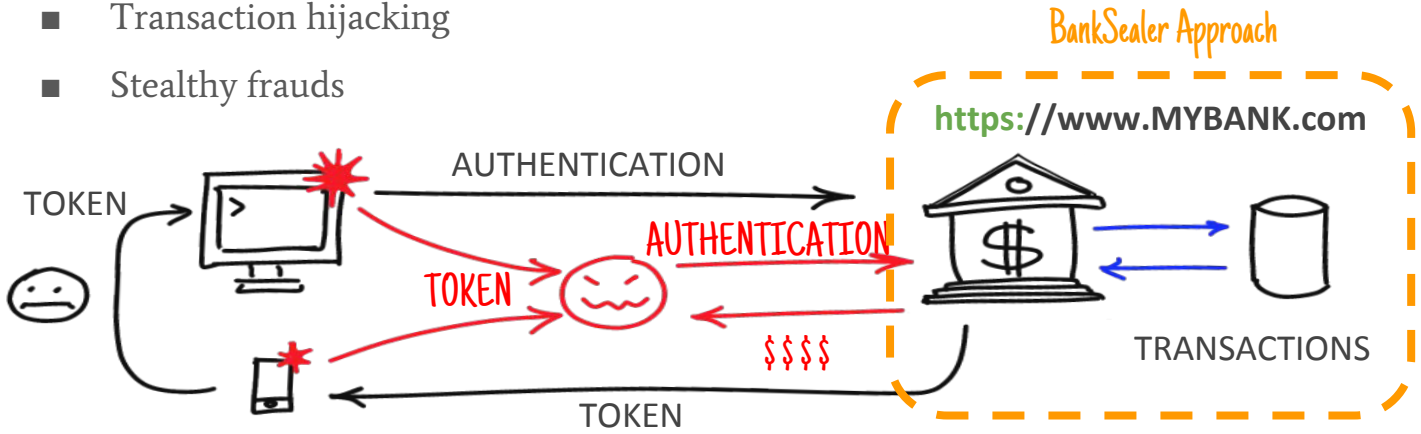
BANKSEALER

FINANCIAL FRAUDS

- Massive growth and adoption of Internet banking services
  - **EU28 Zone:** number of customers doubled from 25% (2007) to 50% (2015) [Eurostat]
  - **Italy:** number of customers grows from 10% (2007) to 30%(2015) [Eurostat]
- Increase of **online banking frauds** and **financial malware attacks**
  - In 2015 almost 2 million users attacked [Kaspersky Security Bulletin 2015]
    - *"Dyre Wolf Banking Malware Stole More Than **$1 Million**"* [IBM Security Intelligence]
    - *"Online attackers steal **£20m** from UK bank accounts"* [BBC]
    - *"Hackers Stole **$300 Million from 100 Banks** Using Carbanak Malware" [Kaspersky]*

FINANCIAL FRAUD SCENARIOS

- Traditional threats
  - Phishing
  - Credentials database compromise
- **Advanced and most prevalent techniques**
  - Man in the browser (MITB) and man in the mobile (MITM) trojans
    - Transaction hijacking
    - Stealthy frauds



BANKSEALER

WHAT ARE OUR COMPETITORS DOING?

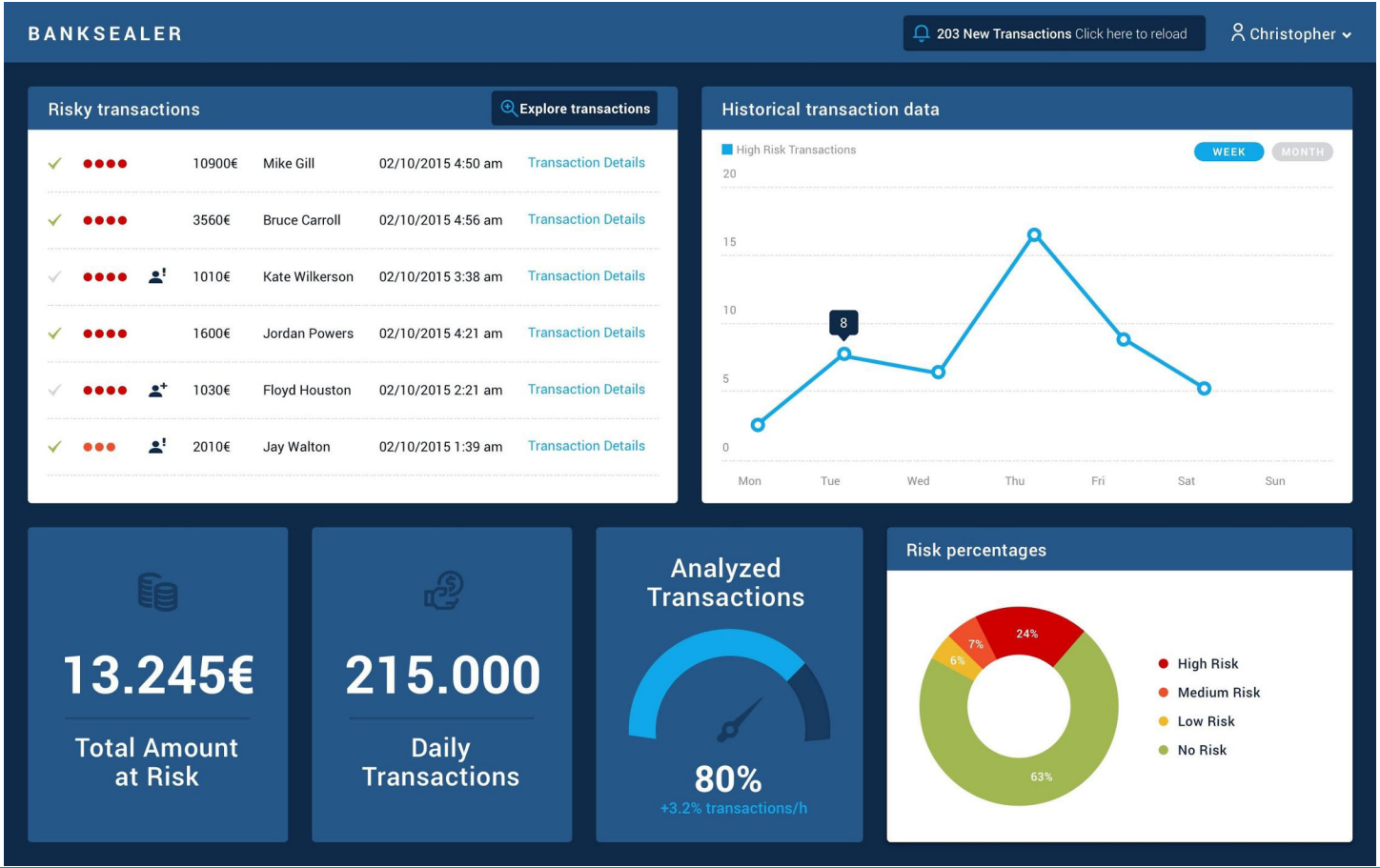
- **Research-wise**
  - Few top-quality works (up to ~60% fraud detection capabilities) with several **limitations:**
    - Work in a **black box** fashion: little explanation attached to the identified frauds
    - **Non-adaptive:** cannot cope with an always-changing adversary
    - Tested only on **synthetic data:** would you deploy one of these tools in your infrastructure?
- **Industry-wise (Falcon, IBM, BAE, Actimize, Palantir - Anti Fraud, Simility)**
  - Large, **complex** products with strong, **same-vendor integration** and data lock in
  - **Horizontal**: claim they can catch **any** type of fraud
  - **Pricey!**

BANKSEALER

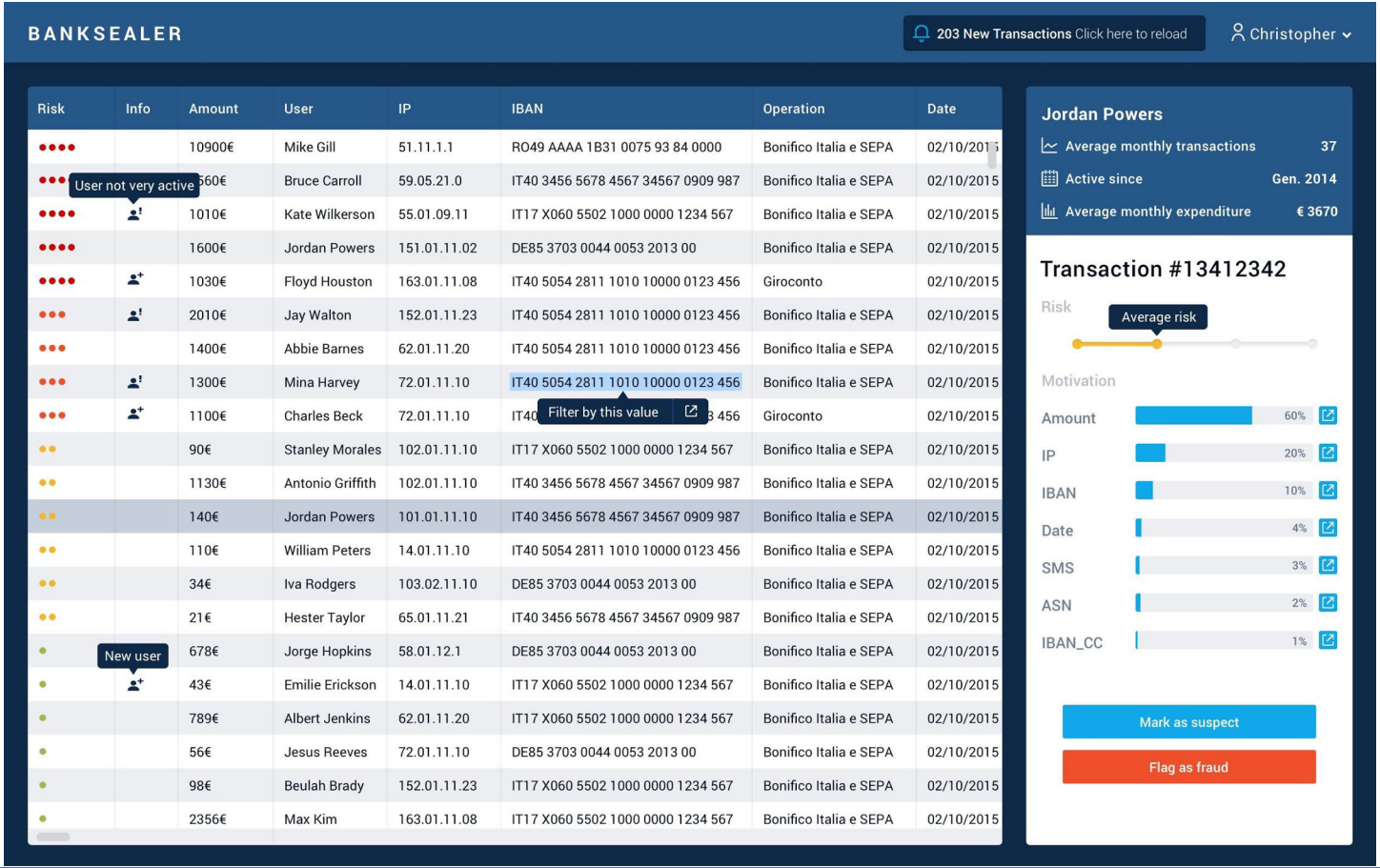
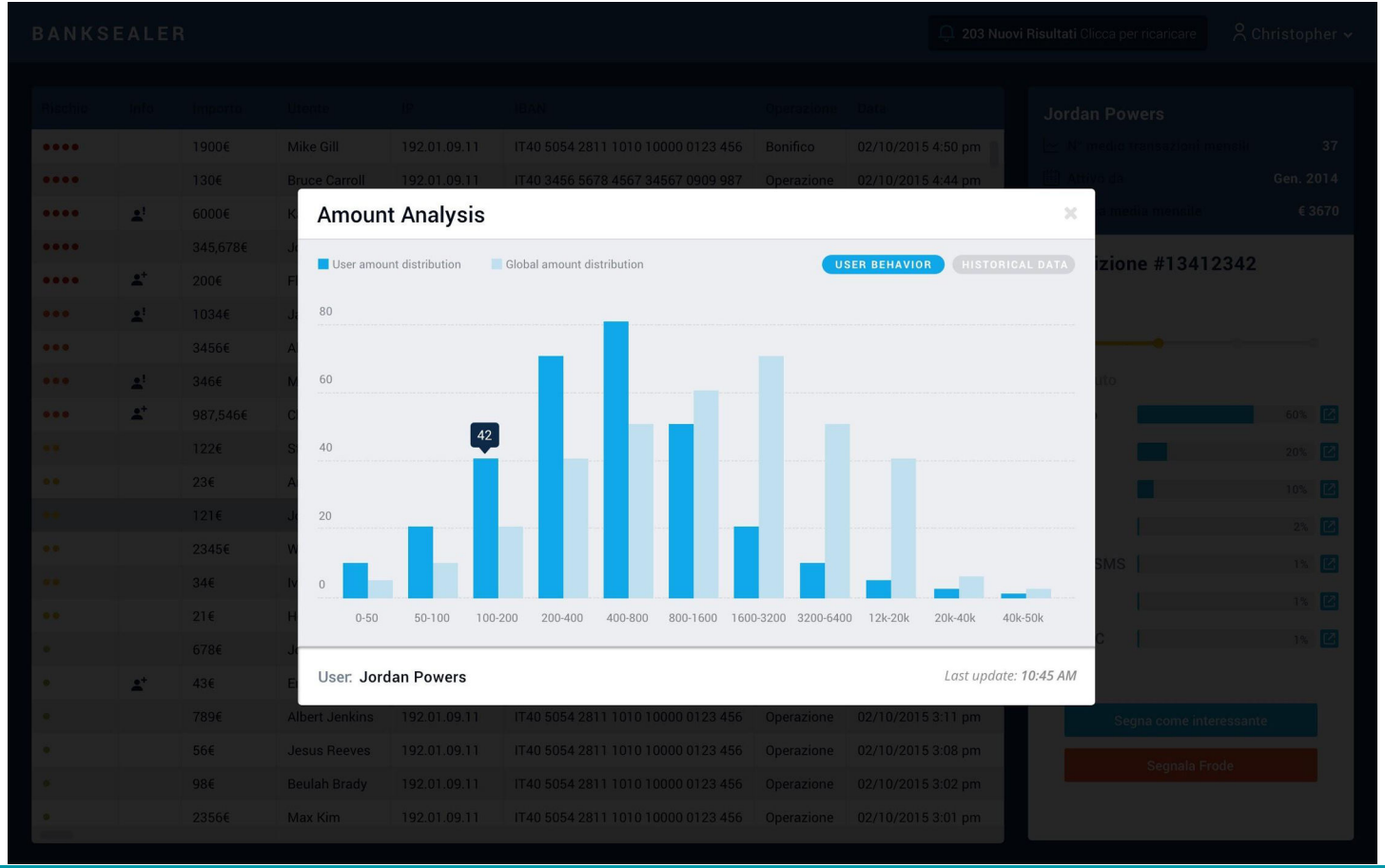
WHAT MAKES BANKSEALER DIFFERENT

- Born as a **research tool**, not a product
  - Focus on **quality** and **scientific** foundation (up to 95% fraud detection capabilities)
  - **Adaptive** by design
  - **White-Box approach:** Easy readable models and results
- Developed in cooperation with one of the **largest national banks**
  - Tested "**in the field**" during development
  - Useful **feedback** that actually **supports the analysts (threat intelligence)**
- Lightweight and **pluggable**
  - Not another IT monster
  - Based on **open formats** and well-defined APIs, can be **easily integrated** into your infrastructure
  - Cross platform: runs on any **operating systems**

THE DASHBOARD



ANOMALOUS TRANSACTIONS



EXPLANATION OF ANOMALIES