Fraud 2.0: the global approach

Remo Marini   UniCredit Business Integrated Solutions – Head of Service Line Security

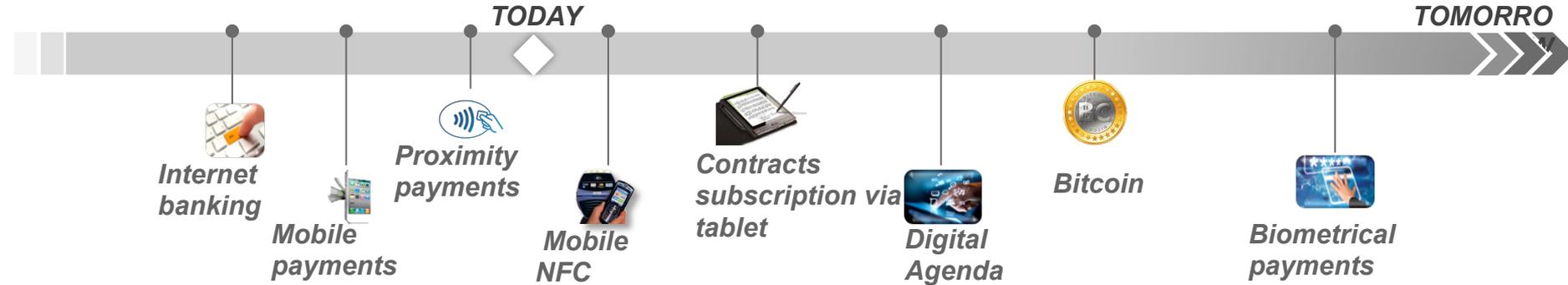**Luigi Altavilla**   UniCredit - [Head of Security Italy

Milan, May 26th

Welcome to **UniCredit**

Official Bank
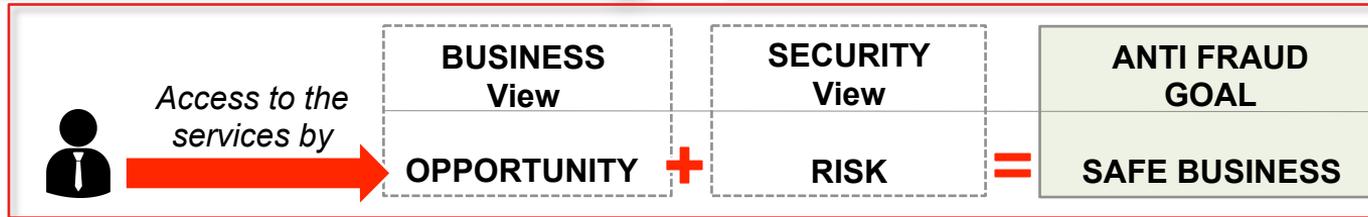
Anti-fraud team UniCredit: a task force committed on fraud
Anti-fraud Solutions - Context

TODAY

TOMORRO

Internet banking

Mobile payments

Proximity payments

Mobile NFC

Contracts subscription via tablet

Digital Agenda

Bitcoin

Biometrical payments

UniCredit is moving toward **services digitalization**. So **the clients** can access to the **business** utilizing **different channels** and can perform **operations in fast and easy** way. **However, the evolution services expose the bank and the clients to new risks.**
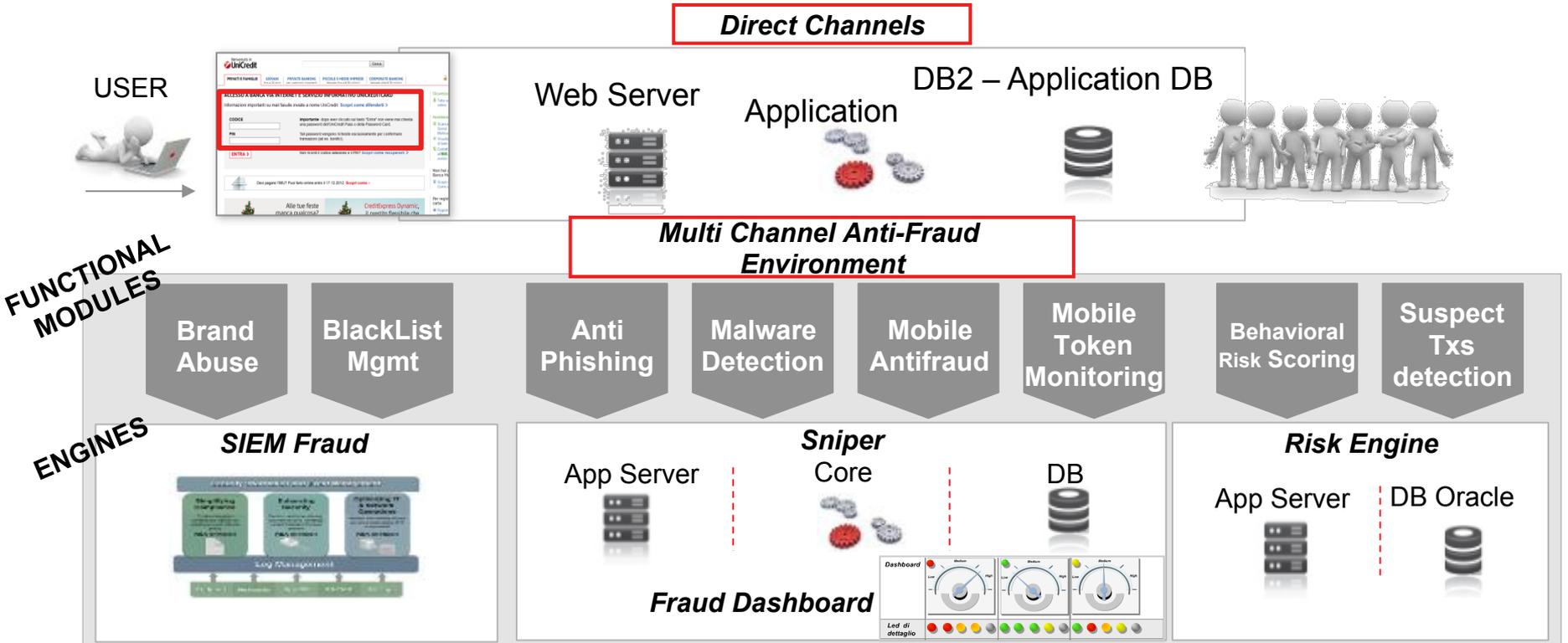
In this context the Fraud management has the goal to guarantee the security of business opportunity

Access to the services by	**BUSINESS View**	**SECURITY View**		**ANTI FRAUD GOAL**
	OPPORTUNITY	**+**	**RISK**	**=**	**SAFE BUSINESS**

Anti-fraud team UniCredit: a task force committed on fraud
Anti-fraud Solutions – Environment

Direct Channels

USER

DB2 – Application DB

Web Server

Application

Multi Channel Anti-Fraud Environment

FUNCTIONAL MODULES

| Brand Abuse | BlackList Mgmt | | Anti Phishing | Malware Detection | Mobile Antifraud | Mobile Token Monitoring | | Behavioral Risk Scoring | Suspect Txs detection |

ENGINES

| *SIEM Fraud* | *Sniper* | *Risk Engine* |

App Server   Core   DB

Fraud Dashboard

App Server   DB Oracle

Anti-fraud team UniCredit: a task force committed on fraud
Anti-fraud Solutions – Approach evolution   1/2

FROM

CORE BANKING

DIRECT CHANNELS

CARDS

TO

Case Management

BIG DATA

INTEGRATED & CORRELATED SYSTEM
UNIQUE LOGIC CROSS CHANNELS

Anti-fraud team UniCredit: a task force committed on fraud
Anti-fraud Solutions – Approach evolution   2/2

The new anti-fraud solution include the evolution from a **reactive** to a **proactive** approach

REACTIVE APPROACH	PREVENTIVE APPROACH

Reactive solutions include **all the solutions that should allow the identification of fraudulent events**:

Transactions monitoring: solutions that allow to define a risk level of transaction and consequently perform certain actions

Information discovery: systems that allow to connect together phenomena, in order to identify abnormal events

Monitoring accesses to databases

Preventive solutions include **all the solutions that should allow to block an attempted fraud before it is successful**:

Fraud prevention: systems that can check whether a certain device is showing abnormal behavior

Behavioral Analysis: systems that analyze the client behavior that access to the web channel

Business Intelligence: data correlation and statistical/predictive analysis

Authentication mechanisms: solutions / mechanisms that protect access to services

Antifraud holistic view: integrated system (cross country, cross LEs), in order to have global vision on frauds phenomenon