Fiorano
Enabling change at the speed of thought

BELLERON
FINANCIAL CRIME FIGHTERS

OPEN BANKING & PSD2 FIGHTING OPEN CRIME

A WHITEPAPER BY BELLERON AND FIORANO

WWW.BELLERON.NET

WWW.FIORANO.COM

THE DICHOTOMY OF OPEN CRIME

Financial innovation, driven by PSD2 and Open Banking will create new and exciting opportunities for customers. It also creates unknown opportunities for criminal activity. In this paper, Belleron and Fiorano will look at this topic from a broad perspective and also discuss questions such as:

What is the impact of Open Banking from a fraud / threat perspective?

- PSD2 forces banks to open up payment and authentication systems. They no longer have exclusive control over customers transactional data-goldmines and payment mechanisms.
- With PSD2 being designed to boost innovation, change market dynamics, drive transparency and competition, and increase participation in the banking and payments industry, what systems are the regulators and industry enforcing and what are the important elements banks need to start thinking about?

Who is impacted by Open Crime?

- This revolutionary opening up of the payment and authentication ecosystem applies to both banks and non-bank actors. Its purpose is to establish a level playing field by harmonizing consumer protection, clearly delineating the rights and obligations of payment providers and their users.
- In this new world, where unproven and new FinTechs or Third Party Payment Providers (TPPs) can offer exciting financial products and services to customers, what roles can customers expect traditional banks to take on and what can banks do to maintain their role as a 'trusted entity'?

Who is accountable: Banks or Third Party Providers?

- With a number of banks viewing PSD2 as a 'competition enabling tax' that is imposed on them, it is not difficult to see many doing the 'bare minimum' to comply.
- While aspects such as SCA, APIs and Dedicated vs. Fallback interfaces have seen much discussion and deliberation, an area overlooked is the allocation of liabilities. How liability gets allocated once access is provided is still a question on many people's minds - between Banks and TPPs, and it's no secret that many banks fear the onus of responsibility will fall on them.

In addition, traditional banks have had decades of under-investment in technology and systems, and often lack the agility required to innovate and fight financial crime. The next few years will see changes to both roles and engagement-stickiness between FinTechs and traditional financial institutions.

Agility is key to success.

SHIFTING THREAT LANDSCAPE
INNOVATION IN FINANCIAL CRIME

The standardized formats and data interchange that PSD2 interfaces enable can provide additional reference points for banks to gain a better understanding of how customers behave and hence more accurately profile and identify fraud related outliers.

The same data points can be available to hostile actors like hackers, criminals, and terrorists who will always follow the path of least resistance, and through Financial Innovation new points of compromise may begin to be found via Third Parties.

PSD2 Transactional Risk Analysis (TRA), Exemption Threshold Values and Fraud Rates

TRA under PSD2 and its application to enforce / exempt specific transactions from SCA depends on elements such as the transaction amount itself, the last time SCA was applied and user device specific characteristics such as the location of the payee/payer, presence of malware and unusual information about the devices used or software on it. Exemptions rely on inputs from transaction monitoring systems based on payment patterns and payment behaviours checked in real-time, including known fraud scenarios and reference fraud rates for each transaction type calculated over a 90-day period.

PSD2 PISPs and AISPs will not have the same risk management culture and systems as banks and are relatively new when it comes to security and safeguarding sensitive data. Banks cannot shy-away from their responsibilities related to their customers' accounts and data, and the those who have invested in traditional fraud identification and combat mechanisms are finding these systems struggle to keep up with the level of innovation in the threat landscape.

FROM APT TO OIT

Belleron sees a very clear paradigm shift coming, moving from Advanced Persistent Threats (APT) to Open Innovation Threats (OIT). How should you understand this shift? Before we dive into describing this shift, let us first have a quick look at the evolution of financial crime.

FINANCIAL CRIME

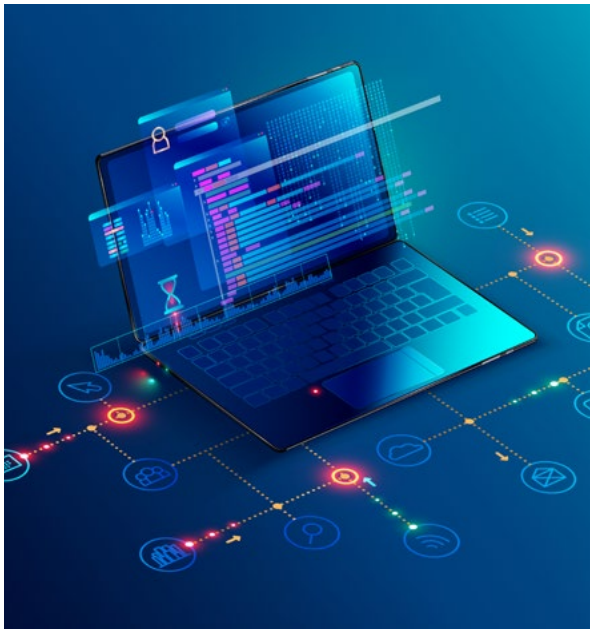
Financial crime has evolved from attacking a single bank account from an individual person to massive and systematic activity involving the hacking of banks and theft from multiple accounts and many people. This activity can result in significant disruption for a bank and can destroy its reputation.

FINANCIAL TERRORISM

We have also seen the development of the next step in financial crime – organized financial terrorism. Terrorists have tried to destroy banks in order to achieve a total disruption of society and the economy. Their first goal is not monetary gain, even though that is a frequent and welcome side effect of their activities. Instead, terrorists want to destroy the banks, economies and way of life of the countries they attack in order to achieve a political, religious or ideological aim. Belleron published a specific white paper on financial terrorism; called **"How to Kill a Bank."**

FINANCIAL INNOVATION

The third step in the evolution of financial crime are criminal opportunities following on financial innovation. Banks no longer control the entire payment process since they have been forced to open up their payment and authentication systems. This provides hostile actors new opportunities to commit crimes. These advanced financial attacks can only be countered with more advanced solutions.



THE PARADIGM SHIFT EXPLAINED

APT vs. OIT in the Open Banking context
Traditional approaches to threats, also known as Advanced Persistent Threat (APT) protection developed from attacking individual personal accounts to massive attacks on multiple accounts.

APT involved financial crime on a larger scale than we were used to, but Open Innovation Threats exists in a world we are not yet familiar with. With the changes PSD2 introduces, banks have to manage risk by organizing security and crime prevention in different ways, being aware of Open Innovation Threats.

Hostile actors are getting smarter, have more time to practice their "art," and are better financed than ever before.

Risk Management by Design
Similar to the impact of Information Security by Design principles on GDPR and Data Protection, Belleron's view and approach to this shift to OIT means that it is now possible to build protection into the open ecosystem by design. This allows banks to and manage related risks better while implementing and supporting innovation.

No one at this point understands the full scope of these changes, however we do know for certain that it will be necessary to manage risk in an extremely open environment. Banks are better off adopting a proactive approach similar to breaking down the walls and doors themselves as hostile actors are trying this anyway.

THE PATH OF LEAST RESISTANCE

Open innovation stimulates hostile actors to be creative and brilliant in as yet unknown ways. It allows criminals to target banks directly by following the "path of least resistance", which may be early start-ups and other consumer facing service providers that interact with banks, all based on PSD2 and Open Banking.

These new kids on the Open-Banking block will also need to create security measures to deal with this paradigm shift, however these may not be available on day 1 and hence these organisations may be prone to making mistakes, making them vulnerable to threats beyond APT.

BELLERON

Fiorano
Enabling change at the speed of thought

FUNDAMENTALS OF OIT

The key aspect of Open Innovation Threats are the unknowns: unheard-of, unperceived, alien, undiscovered, unnamed, unfamiliar, unexplained, unprecedented, bizarre, and exotic threats and attacks.

DETECTION & ANALYTICS
looking for "abnormal-abnormal" behaviour
With Belleron's approach the point of compromise is less relevant then the point of exit. We look at when money is leaving the bank, specifically identifying compromised transactions in a banks huge stream of daily financial events by monitoring "normal-abnormal" behaviour.

This behaviour could be very typical and normal for your bank: everybody buys a new car, goes on a holiday, visits a sports event etc. But what if the entire bank decides to buy a new car at the same time? This is what we call "abnormal-abnormal" behaviour. By segmenting all transactions leaving the bank and counting all its meta data in multiple time-cubes, Belleron looks for sudden data drifts, indicating an unfolding attack.

PREVENTION & RESPONSE
respond to the attack, but keep the bank open
Being able to identify and see data drifts as they happen allows Belleron to initiate protocols that look at the larger picture, and analyse what is happening now and what can explain this "abnormal-abnormal" behaviour the best?

The only appropriate response to OIT is to reroute attacks, doing everything possible not to close down the entire bank or systems; if necessary, a proportional response might involve closing down only a compromised part of the system. Belleron's technology helps keep the bank open in the face of an attack.

CONCLUSION
OPEN BANKING IS HERE TO STAY

Financial OIT is the next generation of financial crime. The kinds of crime that occurred in past banking environments were mostly known. In the new innovative banking environments, we don't fully understand the scope of the possible OIT. The results of these unknown crimes can be massive financial and reputational loss for your company. They must be stopped before getting out of control.

In the OIT environment, you are managing risk while implementing innovation, and by walking this tightrope, you gain many benefits – fuller insight into unknown threats and the effective management of innovation growth.

BUILT IN BY DESIGN

So, it's a new world, a new reality, and a new paradigm. Protection against Open Crime needs to be built in by design. What does this mean? It means that risk monitoring should be a key component of the design, construction and integration of systems. Simply because we don't yet know the nature of the attacks that are coming and in what state you can counter them.

"You should assume you have been compromised and act accordingly. If you set yourself up to manage the risk and manage the scenario in which things go wrong, then you'll be vastly more resilient and in a much better position than if you design a system to make everything totally secure."

Pablo Holmes, a futurist, inventor and ethical hacker at Sibos

FIORANO - SOLUTION PORTFOLIO

Enabling Change
For over two decades, Fiorano Software has been at the fore-front in transforming enterprise backbone infrastructure. With Fiorano, businesses can implement a dynamic strategy to tackle challenges arising from digital transformation projects involving Cloud, IoT and APIs easily. Building on its unique platform, Fiorano continues to deliver banking specific solutions for Core Banking Integration, Bank Digitalisation and of crucial value now, PSD2 Compliance and Open Banking Competitiveness.

A Modern, API enabled Hybrid Integration Platform
Using microservices, a peer-to-peer architecture and high-speed messaging, Fiorano powers real time digital enterprises with advanced Integration and API Management capabilities, leveraging the best of systematic (centralized, high-control) and adaptive (federated, high-speed) environments.

PSD2 Accelerator
A ready-to-deploy technology infrastructure that helps banks rapidly comply with API publishing obligations under the PSD2 to meet deadlines. Fiorano's PSD2 Accelerator includes all the technology banks need in a pre-integrated stack that is pre-configured to global API specifications including Open Banking UK (OBIE), Berlin Group NextGenPSD2, STET and Hong Kong (HKMI).

Core Banking Integration
Fiorano's core banking integration technology supports codeless integration and with multiple out of the box connectors for multiple core-banking systems allows drag-and-drop connection, distribution and execution of business logic for bank digitisation and service enablement.

BELLERON - SOLUTION PORTFOLIO

Belleron's solution portfolio began with fighting financial crime and has now moved to countering financial terrorism and financial innovation. Belleron serves in all three of these domains, implying various solutions based on proprietary methods and technology.

SECURE®
Belleron deploys its expertise through its SECURE® method. Using this method, we fill gaps in customers' knowledge and lack of implementation expertise in the area of information security. The Belleron consulting team, equipped with the Belleron SECURE® method, ensures that its customers benefit from the availability of highly trained experts. This expertise and method has been incorporated into the world of Belleron Solutions.

CAPTURE®
In order to provide solutions for financial crime, financial terrorism and financial innovation, Belleron has built CAPTURE®. It adds a new dimension to risk management and security fighting APT and will future-proof our customers against OIT. There is much more regulation to come, and the increasingly open environment forced onto banks must be defended.

CAPTURE is the Operating System for FUSION CENTERS to protect financial institutions against massive attacks where thousands of accounts are compromised. It is a holistic cross account transaction monitoring system, CAPTURE® adds a new dimension to risk management and security fighting Advanced Persistent Threats (APT) and will future-proof our customers against Open Innovation Threats (OIT) emerging from PSD2, OpenBanking and Faster Payments. There is much more regulation to come, and the increasingly open environment forced onto banks must be defended.

AUTHORS

Biju Suresh Babu
Lead - Open Banking
Fiorano software

Bas Uildriks
Managing Director
Belleron

Fiorano
Enabling change at the speed of thought

BELLERON
FINANCIAL CRIME FIGHTERS

WWW.FIORANO.COM

WWW.BELLERON.NET