


[Home](#)
[Resources](#)
[Articles](#)

The Risks of Open Banking Fraud and How to Protect Yourself in 2023



Last Updated: February 09, 2023 by Bence Jendruszak

Table of Contents

[Products](#)[Use Cases](#)[Resources](#)[Developers](#)[Company](#)[Pricing](#)[Start free](#)[Get a demo](#)[Login](#)

FollowUs!



info@seon.io +44 20 3997 6090

© Copyright SEON Technologies Ltd. - [Legal & Security](#)

Fintechs and neobanks benefit greatly from the API ecosystem. However, they also open banking fraud risks involved. Let's see how that may impact your operations at your organization.

What Are the Uses of Open Banking?

Open banking is designed to create a bridge between people's financial information and third-party services. It is a solution to the historical problem of banks regarding customer data. The EU (and now an increasing number of regulatory bodies) created open banking so that more third-party companies can offer their services to banking customers.

While the UK has taken the lead in open banking initiatives, other countries are following suit.

The Payment Services Directive (PSD2) and General Data Protection Regulation (GDPR), are driving Europe towards an open banking standard. The US, LatAm, and Asia are also toying with their own versions.

According to [Payper's Open Banking Report](#), 87% of all analyzed countries surveyed said they had open banking initiatives in readiness.

What Are the Benefits of Open Banking?

Open Banking is a user-centric process. It allows customers to access a wider range of financial products and services that are tailored to their needs, by breaking up the monopoly of banks. It can reduce the need for KYC checks each time you purchase a financial product (mortgage, loan, credit card, etc). You can also gain access to more products and services.

For fintech companies, open banking makes it easier to target customers who would have otherwise been tethered to a bank's financial services. Banks and traditional financial institutions can partner with agile startups that can provide more interesting features to their pre-existing customers.



Speed up access to financial services.

Modern banks, especially challenger banks and neobanks who the on-demand generation, have built entire business models o experience.

Examples of Open Banking

Open banking enables a variety of products and services relate



Digital Identity

Identity networks and hubs connect retail and banking by provi identity. In short, they leverage Know Your Customer and Custc Diligence processes that banks already performed to demonstr user's identity is valid. Third-party services also aim to decoupl financial information, so that ID data is kept secure elsewhere.



Finance Management

A growing number of services offer bank account aggregators, customers control all their accounts from one app dashboard o



Product Matching

From mortgages to loans and even overdrafts, there is no short that take advantage of open banking APIs to offer tailored prod customers.

What Is Open Banking Fraud?

Open banking fraud sees bad agents take advantage of open banking to exploit financial products, services, and customer information. It is growing at an alarming rate, simply by virtue of introducing new points of failure between financial organizations and users. Fraudsters are also adept at exploiting new technologies, which open banking meets the definition for.

Products

Use Cases

Resources

Developers

Company

Pricing

Start free

Get a demo

Login

FollowUs! 👍



info@seon.io +44 20 3997 6090

© Copyright SEON Technologies Ltd. - [Legal & Security](#)


[Products](#)
[Use Cases](#)
[Resources](#)
[Developers](#)
[Company](#)
[Pricing](#)
[Start free](#)
[Get a demo](#)

The Risks of Open Banking Fraud

Sadly, **open banking risk may sometimes overshadow its benefits**. While the technology may also put organizations at risk. This is due to several factors:

[Login](#)

Larger Ecosystem = More Risk

An open banking ecosystem may include various players such as providers, third-party providers, customers, regulators, and government agencies. That's a lot of potential points of failure for data security. Fraudsters are adept at targeting the weakest link in a chain.

[FollowUs!](#)

info@seon.io +44 20 3997 6090

 © Copyright SEON Technologies Ltd. - [Legal & Security](#)

Account Takeovers Bring Higher Rewards

As we know, accessing banking information is the holy grail for fraudsters. They are adept at mining every account they infiltrate for personal data as well as currency, reward points, or crypto.

In the context of ATO fraud, the problem of linked accounts via APIs is evident: losing control of one account could mean losing much more. Customers' ID documents or card numbers could end up in the wrong hands where they will fuel synthetic identity fraud transactions.

One Bad Apple Spoils the Lot

If all these services are connected by one technology (the API), they are essentially at the mercy of the initial KYC check. What happens if someone has successfully bypassed it? You have an infiltrator who can access all accounts, apply for loans, take out a mortgage, and essentially scam every partner involved.

The problem is exacerbated **when it comes to AML compliance**. If one money launderer manages to enter through the front door for one fraudulent transaction, who gets blamed by the government bodies? That is to say: who will pay the massive financial crime fines that inevitably result from failing to meet AML in banking requirements?

Single Point of Attack

Even if banks' security is watertight, what happens when every interconnected service offers the same single point of attack? Security and data protection hygiene are increasingly important in the API economy. **Open banking fraud would give hackers and fraudsters a potentially higher reward.**

Information and Security Asymmetry

Last but not least, there is something to be said for the false sense of security that open banking APIs may create. It's not unlike a digital version of the bystander effect, where organizations are less likely to verify data when they trust it comes from a reliable source.



careful handling of personal information to pass a KYC check. If you go down on the verification, you are likely to open a backdoor into criminals.

How to Prevent Open Banking Risks

Open banking risk can be anticipated and prevented using the following methods:

- **Secure your data at all stages:** The more data gets shared, the more failures are introduced. It's of the utmost importance that you follow the best data protection guidelines, going above what meet compliance requirements.
- **Verify IDs in more ways than one:** ID proofing, or identity verification, is becoming the battleground where companies win or lose the battle against fraudsters and cybercriminals. You should implement as many measures as you feel comfortable with, such as biometrics, multi-factor authentication (2FA), and digital footprint analysis.

Webinar Highlights 11: 5 Reasons to Use Social KYC & D



- **Vet companies your customers rely on:** Are customers signing up for BNPL services by the day? Taking out loans with fast loan providers could do worse than to perform due diligence checks on the services.

Takeaways

Open banking is a response to customer demand for more choice and a better, frictionless user experience. By sharing data via APIs, fintech companies, third-party service providers, neobanks, and challenger banks can offer personalized products.

The key, however, is that customers need to have trust in these organizations and in the security of their data ecosystems. And there is no surer way to lose trust than to allow one bad agent into your ecosystem, especially if they can then exploit the whole lot with one attack only.

We believe that open banking risk and open banking fraud can only be reduced if every organization takes the **financial risk management**, the risk assessment and fraud detection into their own hands.

Open Banking Fraud FAQ

Products

Use Cases

Resources

Developers

Company

Pricing

[Start free](#)
[Get a demo](#)


Login

FollowUs! 🍷



info@seon.io +44 20 3997 6090

© Copyright SEON Technologies Ltd. - [Legal & Security](#)



information to be accessed by third-party companies.




What are the risks of open banking?


Open banking adds more points of failure where customer data is shared. The more data is shared between third-party companies and financial institutions, the more risk there is that the data could fall into the wrong hands.

Is open banking disruptive?

Yes. Historically, financial institutions guarded their customers' information closely. But thanks to open banking, these large companies are now sharing information with smaller, more agile third-party companies providing services and products.

Share article





Products

Use Cases

Resources

Developers

Company

Pricing


Start free

Get a demo

Articles

ARTICLE


Financial Fraud Detection and Prevention: Best Approaches in 2023







April 06, 2023 by Eric Gressman

Everything you need to know about the best approaches to detecting and preventing financial fraud.

Login

FollowUs! 



info@seon.io +44 20 3997 6090

© Copyright SEON Technologies Ltd. - [Legal & Security](#)

See a live demo of our product

[Click here](#)

Bence Jendruszak

Bence Jendruszák is the Chief Operating Officer and co-founder of SEON. Thanks to his leadership, the company received the biggest Series A in Hungarian history in 2021. Bence is passionate about cybersecurity and its overlap with business success. You can find him leading webinars with industry leaders on topics such as iGaming fraud, identity proofing or machine learning (when he's not brewing questionable coffee for his colleagues).

Use cases

<https://seon.io/resources/open-banking-risk-and-fraud/#:~:text=What are the risks of,fall into the wrong hands.>

5/7

SEON Resources

 Search



Articles



Podcasts



Webinars



Case Studies



Videos



Dictionary



Guides



Comparisons



Events

Products

Use Cases

Resources

Developers

Company


Pricing

Start free

Get a demo

Login

FollowUs! 

info@seon.io +44 20 3997 6090

© Copyright SEON Technologies Ltd. - [Legal & Security](#)


Sign up for our newsletter


The top stories of the month delivered straight to your inbox

Email

Subscribe

We look after your data - for more information, please review our Privacy Policy.


 SEON


Fraud Fighters 


e: info@seon.io p: +44 20 3997 6090 [Contact Us](#)


 CROWD  4.7  Capterra  4.9


NAVIGATION
















© Copyright SEON Technologies Ltd. - [Legal & Security](#).

Made with  in Budapest, London, Austin & Jakarta



Products

Use Cases

Resources

Developers


Company


Pricing


Start free


Get a demo


Login

FollowUs! 









info@seon.io +44 20 3997 6090

© Copyright SEON Technologies Ltd. - [Legal & Security](#).