

# SECURITY AND COMPLIANCE IN OPEN BANKING

KEY SUBJECTS INCLUDE

- // Open banking use cases
- // How banks plan to deliver on open banking
- // Security challenges that come with open banking
- // How to stay open-banking compliant
- // Building compliance and security solutions in-house versus choosing a provider

AUTHORS

**Bruno Cambounet,**  
Head of research  
at Sopra Banking Software

**Yann Metz-Pasquier,**  
General manager for NEO  
at Sopra Banking Software

# SECURITY AND COMPLIANCE IN OPEN BANKING

Open banking is just one example of how the banking world has changed in recent years. It has fast become a vital component of how a modern bank needs to behave in order to meet the needs of today's banking customer. And unless they adapt quickly to reach basic capabilities such as digital identity services and KYC process automation, banks will be unable to offer their customers the latest added value financial services use cases.

However, offering best-in-class open banking or open finance use cases is easier said than done. To do so, banks need to ensure that they are open banking compliant, and that they have the security infrastructure in place to protect customer data.

By leveraging data taken from our [2021 digital banking experience report](#) – conducted with Sopra Steria and Forrester Consulting – we look at how banks are increasingly adopting open banking practices, as well as steps they're taking (or, at least, planning to take) to remain secure and compliant.

01

---

THE RISE OF OPEN BANKING

02

---

BANKS DELIVERING ON OPEN BANKING

03

---

STAYING SECURE

04

---

COMPLIANCE ACTING AS A CATALYST

05

---

STAYING IN-HOUSE OR SEEKING THIRD-PARTY HELP

06

---

THE FUTURE IS OPEN. BANKS NEED TO BE READY

01 THE RISE OF OPEN BANKING

02 BANKS DELIVERING ON OPEN BANKING

03 STAYING SECURE

04 COMPLIANCE ACTING AS A CATALYST

05 STAYING IN-HOUSE OR SEEKING THIRD-PARTY HELP

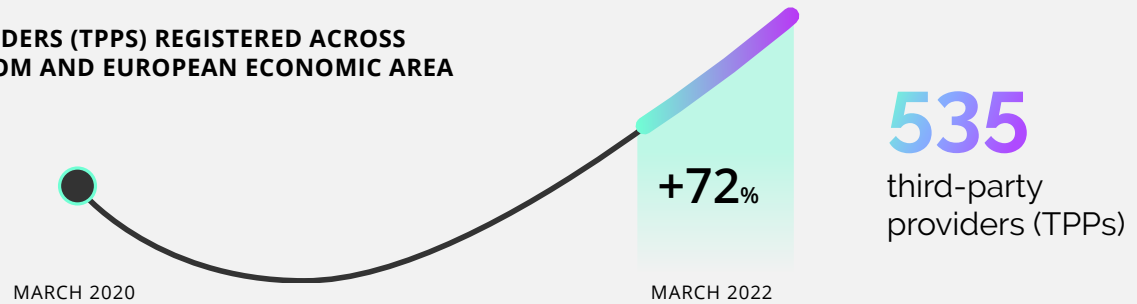
06 THE FUTURE IS OPEN. BANKS NEED TO BE READY

# THE RISE OF OPEN BANKING

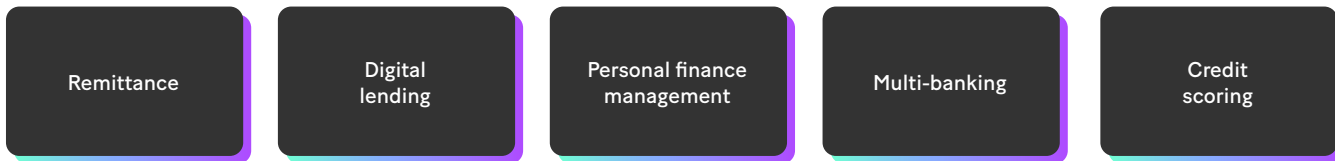
January of this year marked four years since the new Payments Service Directive 2 (PSD2) came into force, and its impact has been more prominent than many experts previously predicted. 83% of financial executives say that it has had a revolutionary impact on the industry. Indeed, the ripple effect has been far and wide.

As of March 2022, there were 535 third-party providers (TPPs) registered across the United Kingdom and European Economic Area – a two-year growth of +72%.

## THIRD-PARTY PROVIDERS (TPPS) REGISTERED ACROSS THE UNITED KINGDOM AND EUROPEAN ECONOMIC AREA



And the result has been a proliferation of open banking-powered use cases.



End-consumers have had a taste of what open banking can offer, and they want more. The question is: Are banks able to deliver?

Data taken from research conducted by our partners Tink. [Click here to read the full report, The open banking revolution](#)

01 THE RISE OF OPEN BANKING

02 BANKS DELIVERING ON OPEN BANKING

03 STAYING SECURE

04 COMPLIANCE ACTING AS A CATALYST

05 STAYING IN-HOUSE OR SEEKING THIRD-PARTY HELP

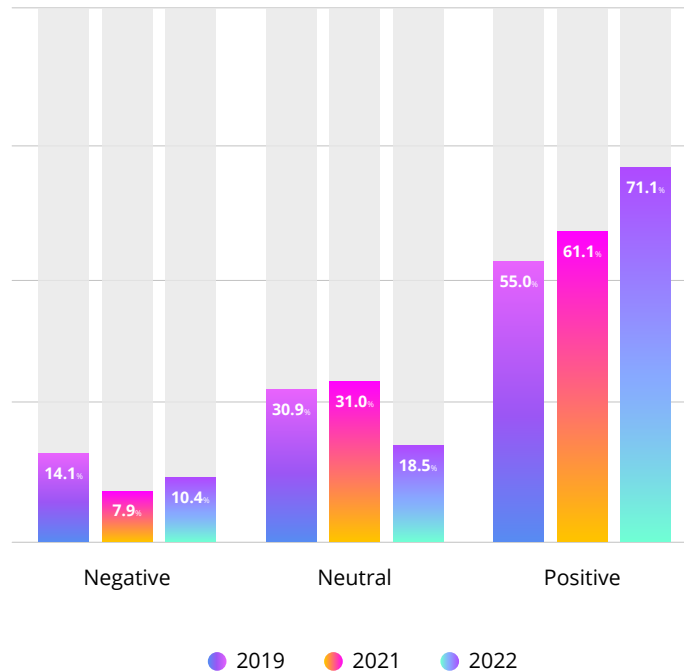
06 THE FUTURE IS OPEN. BANKS NEED TO BE READY

# BANKS DELIVERING ON OPEN BANKING

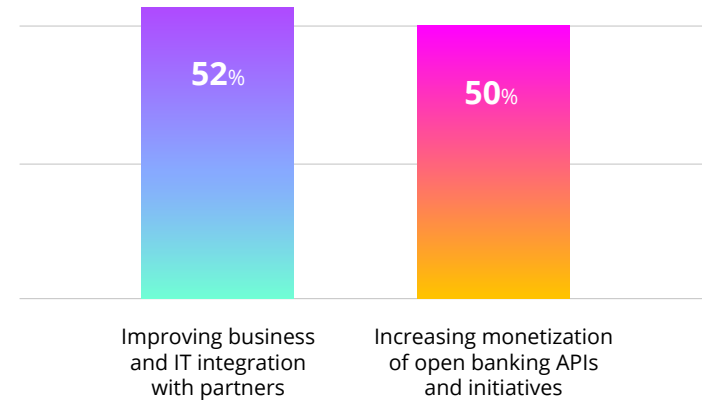
The attitude among banks toward open banking has shifted significantly since PSD2. Indeed, financial services executives are more positive about open banking and its impact than ever before.

Per research conducted between Sopra Steria and Forrester Consulting, banks are increasingly keen to leverage open banking. However, it is new territory for many of them.

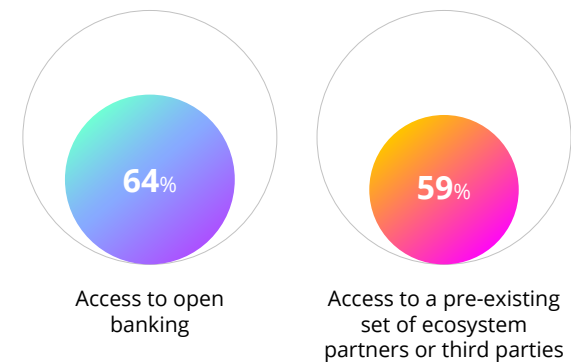
WHAT IS YOUR GENERAL ATTITUDE TOWARD THE OPEN BANKING MOVEMENT



TOP PRIORITY INITIATIVES EXPECTED TO DRIVE THE HIGHEST GROWTH



"VERY IMPORTANT" OR "CRITICAL" NEEDS



01 THE RISE OF OPEN BANKING

02 BANKS DELIVERING ON OPEN BANKING

03 STAYING SECURE

04 COMPLIANCE ACTING AS A CATALYST

05 STAYING IN-HOUSE OR SEEKING THIRD-PARTY HELP

06 THE FUTURE IS OPEN. BANKS NEED TO BE READY

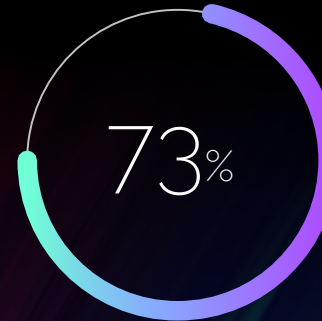
# STAYING SECURE

While open banking (and open finance to a larger extent) represents a huge opportunity for banks and the wider financial services industry, it also poses issues around security. Indeed, the rate of fraud and data breaches is expected to rise to an all-time high, and API attacks could be a big part of that.

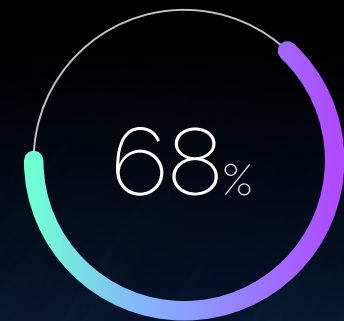
Equipped with the right infrastructure and experience to manage security risks, banks are well prepared. And, per our research, they're already aware of the task at hand.



Security concern is the biggest challenge with regards to developing a digital ecosystem of products and services **for 42% of banks' respondents.**



**For 73% of banks' respondents,** improving security is considered either a "high priority" or a "critical priority"



**For 68% of banks' respondents,** improving fraud management is considered either a "high priority" or a "critical priority"

## HIGHEST RANKING INITIATIVES

*Improving security*



*Improving risk management and control*



01 THE RISE OF OPEN BANKING

02 BANKS DELIVERING ON OPEN BANKING

03 STAYING SECURE

04 COMPLIANCE ACTING AS A CATALYST

05 STAYING IN-HOUSE OR SEEKING THIRD-PARTY HELP

06 THE FUTURE IS OPEN. BANKS NEED TO BE READY

# COMPLIANCE ACTING AS A CATALYST

The PSD2 Directive triggered the need for banks to quickly adapt and prepare for potential threats while integrating into the digital ecosystem. Banks and financial institutions that are unable to keep up-to-date will find themselves losing ground to competitors.

Below are some of the standards and moving parts that banks need to be compliant with to be safe and successful in open banking.

THE *Berlin* GROUP   
A EUROPEAN STANDARDS INITIATIVE  
*Berlin Group NextGenPSD2  
 for EU countries*

 OpenID®  
*Open ID Foundation &  
 Financial Grade API*

  
*Strong Customer  
 Authentication*

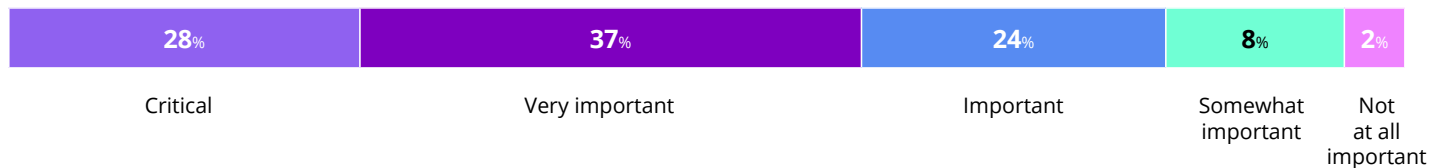
  
*TPP Authentication and  
 Authorization - EIDAS*

  
*Customer consent  
 management*

  
*Secure transactions  
 and information*

Our research shows that these are key concerns for banks when entering the digital ecosystem. More than two-thirds of banks' respondents said that security by design and compliance with all legal and security-driven requirements was either "Very important" or "Critical".

**WHEN YOU CHOOSE A THIRD-PARTY VENDOR TO WORK WITH TO ENABLE YOUR DIGITAL ECOSYSTEM, HOW IMPORTANT ARE SECURITY BY DESIGN AND COMPLIANCE WITH ALL LEGAL AND SECURITY-DRIVEN REQUIREMENTS?**



01 THE RISE OF OPEN BANKING

02 BANKS DELIVERING ON OPEN BANKING

03 STAYING SECURE

04 COMPLIANCE ACTING AS A CATALYST

05 STAYING IN-HOUSE OR SEEKING THIRD-PARTY HELP

06 THE FUTURE IS OPEN. BANKS NEED TO BE READY

## STAYING IN-HOUSE OR SEEKING THIRD-PARTY HELP

The question for many banks is how to become secure and compliant in open banking. But the answer is not always straightforward.

Per our research, over a third of banks are working on an in-house compliance solution, and half are working on their own enhanced data security solution. However, experience suggests that many in-house solutions struggle, especially when it comes to innovation and creating a smooth customer experience.

### HOW DO BANKS PLAN TO INVEST IN DATA SECURITY OVER THE NEXT 12 MONTHS?

|                               |     |
|-------------------------------|-----|
| Outsource to another provider | 40% |
| Build ourselves               | 47% |
| No plans to invest            | 10% |
| Don't know / does not apply   | 3%  |

### HOW DO BANKS PLAN ON DELIVERING OPEN BANKING COMPLIANCE?

|  |     |
|--|-----|
| Source exclusively from a third party        | 23% |
| Augment existing services with a third party | 37% |
| Build in-house                               | 33% |
| No plans to deliver / invest                 | 5%  |

## Sopra Banking Software's off-the-shelf **Open Banking Compliance Solution**

means that banks can become fully PSD2 compliant in just five days, without changing their back-office infrastructure. It also provides security features that includes customer authentication, PSU consent management and TTP management,

[FIND OUT MORE](#)



# THE FUTURE IS OPEN. BANKS NEED TO BE READY

Open banking is just the start for banks and the financial services industry. Those on the forefront are already preparing for the next stage: open finance, where the opening up of data extends beyond just banking to finance and insurance.

Clearly, the future is open, and banks need to be ready for that. Becoming open-banking compliant should be considered a vital starting point, allowing banks to offer the latest products and services, as well as a world-beating customer experience.

Moving forward, banks and financial institutions need to be increasingly adaptable to meet the ever-changing needs of the market, able to adjust rapidly to be compliant with new regulations, advances and technology requirements. Doing all of this alone could be a daunting prospect, and those that succeed may well be the banks that decide to seek out the expertise of experienced partners.



Sopra Banking Software is the partner of choice for more than 1,500 financial institutions worldwide. The rich variety of our solutions, the strength of our conviction and our passion for innovation enable us to support our clients on a daily basis and in their future projects, as well as in their goals regarding financial inclusion. Our customers, based in over 80 countries around the world, benefit every day from our technologies and software, as well as the expertise of our 5,000 employees. Sopra Banking Software is a subsidiary of the Sopra Steria Group, a European leader in consulting, digital services and software development. With more than 47,000 employees, the Sopra Steria Group generated a turnover of €4.7 billion in 2021.

*To find out how we can help your bank to create market-beating digital transformation strategies, visit [www.soprabanking.com](http://www.soprabanking.com) or contact us at [hello@soprabanking.com](mailto:hello@soprabanking.com)*

