DATA SECURITY IN OPEN BANKING

Dispelling myths and misconceptions

```
httpås://api.sandbox.yts.io/v1/users
rtification.pem\
vate-key.pem\
tent-Type: application/jtpsd" \
```

```
openssl req - out tls-csr.pem -new -newkey rsa:4096 -nodes -keyout tls-private-
```

```
REQUEST_TOKEN=$(step crypto jwt sign--iss $CLIENT_ID \
-- kid $REQUEST_TOKEN_PUBLIC_KEY_ID \
-- key private-key.pem \
-- alg RS512 \
-- jti= 'uuidgen' \
-- subtle)
echo $REQUEST_TOKEN
```

```
-- header "Content-Type: application/json" \
-- header "Authorizaztion: Bearer $ACCESS_TOKEN"
-- data "{\"redirectUrl": \"$REDIRECT_URL\"
-- header "PSU-IP-Address: ff39:6773:c03c48e8:5\
```

YTS | Yolt Technology Services

YTS

Yolt
Technology
Services

YTS (Yolt Technology Services) provides open banking expertise and services to other organisations through a single and secure API - building, managing and maintaining Account Information Services (AIS) and Payment Initiation (PIS) connections, alongside Data Enrichment and Know Your Customer (KYC) services, for top financial institutions and ambitious tech businesses.

Launched in 2018, YTS offers the most comprehensive open banking service to companies on a scale no other competitor can match. In October 2020, YTS became the first Open Banking provider to reach 1 billion API calls, averaging over 26 million API calls every week, with its API coverage accounting for 95% of bank accounts in the UK, as well as 90% in the Netherlands and France, and 80% in Italy, Spain, and Belgium.

From the very beginning, YTS worked closely with the Open Banking Implementation Entity (OBIE), other TPPs and financial institutions has shape and launch open banking in the UK and was recently recognised as the Alt-Fi Open Banking Provider of the Year in their 2020 awards.

YTS' API technology has also powered the Yolt App since its inception, and YTS recently launched as a separate but connected business. YTS works both independently of and simultaneously with the Yolt App, with its APIs still powering the platform, and is now expanding into the open banking service provider market. The combined group is led by Nicolas Weng Kan, creating a cohesive overall strategy and ensuring that both businesses are evolving in the same direction.

OUR SERVICES

ACCOUNT INFORMATION SERVICES (AIS)

Strengthen your business by importing transaction information (AIS data) straight from the bank for accurate analysis, actionable insights and risk reduction.

PAYMENT INITIATION SERVICES (PIS)

Expand your offering by allowing your customers to transfer money and pay for purchases directly from within your bank account, all while reducing costs and risk.

DATA ENRICHMENT

Increase the value of your AIS data with data enrichment, and get even more out of your YTS open banking connections.

DATA SECURITY IN OPEN BANKING

Dispelling myths and misconceptions

Introduction – Roderick Simons, Chief Technology Officer, YTS

Over the last 50 years, the banking industry has seen many innovations that have revolutionised how we engage with money. The introduction of cash machines, telephone and internet banking, debit cards, and digital payments have all changed the way we interact with our finances, while the introduction of contactless payments just over a decade ago has reduced the use of physical currency as a form of payment and moved us closer to becoming a cashless society.

The advent of the second Payment Services Directive (PSD2) in January 2018 aimed to revolutionise the market even further by opening up the financial services industry and putting power into the hands of consumers. The initiative was designed to bring more transparency, competition and innovation into the financial services industry, creating an opportunity for people and businesses to use their transactional data, shared via secure application programming interfaces (APIs), to access better products and services – known as Account Information Services (AIS). More recently, Payment Initiation Services (PIS) are being used to transform the way businesses and consumers conduct transactions, using these APIs.

There are currently close to three million people in the UK using some kind of open banking service, rising by over one million users in under a year. In other countries, too, open banking is growing – in Italy, for instance, 8 million open banking API calls were made between July and September 2020. The increasing global shift to open banking usage is a promising indicator for the future and the perfect foundation for the potential use of a broader open finance model.

Open finance would see open banking APIs used to cover a broader range of financial products such as savings accounts, mortgages and pensions. It would expand the current limited scope of payment accounts to one that is more inclusive and allow people to have the option to manage their entire financial footprint digitally. However, while open banking innovation and the increased availability of APIs has enticed early adopters, there is still a lot to be done before we are able to reach an open finance framework.

Yolt Technology Services (YTS) recently surveyed 800 business leaders in sectors across the financial services industry in both the UK and the Netherlands to understand the role of data security issues in the open banking ecosystem. The research showed would-be open banking adopters have questions and uncertainties around data security, data sharing, and the open banking model.

YTS found a significant portion of respondents felt better education and training (42%) and increased guidance from regulators (42%) would be the best way to alleviate business fears about the data security risks of open banking adoption. The current general regulatory environment was also perceived by almost one in five respondents (17%) as the greatest risk to widespread adoption of open banking.

To maximise open banking's potential, more needs to be done at a regulatory level to educate businesses and consumers about its inherent data security controls. Better guidance from regulators could also help change how many businesses currently perceive the regulatory environment.

Greater regulatory support would also ensure all companies are held to account when it comes to the delivery, availability and performance of the API and the data within. This support is essential for creating a collaboratively developed and, therefore, richer open finance ecosystem.

BREAKING DOWN THE BARRIERS FOR ADOPTION OF OPEN BANKING

– Roderick Simons, Chief Technology Officer, YTS

One of the main barriers to the adoption and growth of open banking is the common lack of understanding of open banking within the wider ecosystem, as demonstrated by YTS' 'Unlock the Value of Open Banking' report.

Even within financial services companies themselves, understanding of open banking is not always correct. For example, a customer might call their bank to ask if they can share their data with a trusted and authorised Third-Party service Provider (TPP), and the response from the bank employee could be that they should never share their data. For good reason, this has been the general stance adopted across the industry for many years, but it's important to know that open banking was designed with security and control for customers as a central pillar.

It's possible that concerns have arisen because of the role that screen-scraping has previously played in the data sharing process. It's true that with screen-scraping, banking credentials are stored with another business and cannot be easily recalled, giving the consumer less control over their data. However, the UK's open banking infrastructure is designed to operate solely through API-powered sharing, and many providers have subsequently moved away from screen-scraping. Strong Customer Authentication (SCA) is producing a similar effect in other countries. YTS itself has not relied on screen scraping for some time, and all of our data collection methods are API based and at the highest level of security.

Such examples of mixed messaging around screen-scraping vs API-powered sharing do not help to address the misconceptions around open banking, nor do they encourage further adoption, but the data reveals that this is down to how businesses perceive the risks at a basic level.

A clear split emerged between respondents on whether they think data security is a business risk or customer risk. 48% believe it to be a business risk, as open banking requires organisations to take ownership of and responsibility for large amounts of financial and personal data, and this can result in a costly fine should anything go wrong.

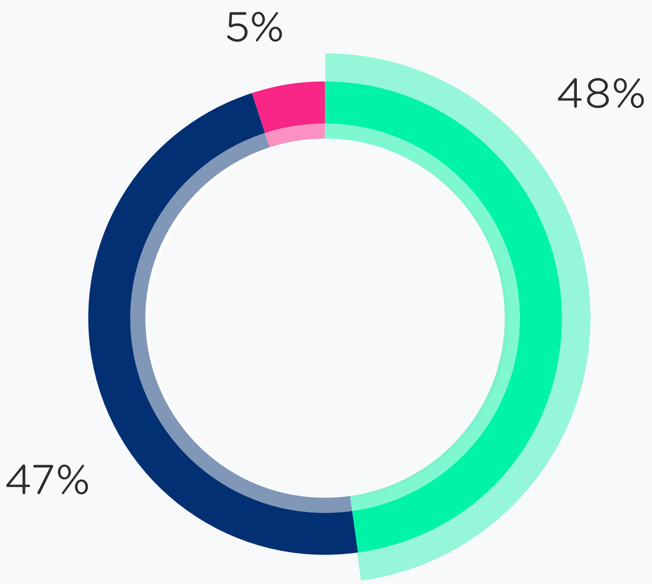
On the other hand, 47% think that the data security risk is more a customer risk, because open banking is a new service that customers are unfamiliar with, which might make them unlikely to want to share the necessary amount of data. Interestingly, survey respondents from the Netherlands and the UK had opposing views on this subject – 58% of respondents in the Netherlands falling in the customer risk camp compared to 59% of UK respondents feeling that business risk most closely defined the risk of open banking to data security.

Q1. WHICH OF THE FOLLOWING CATEGORY MOST CLOSELY DEFINES THE RISK TO DATA SECURITY POSED WITH OPEN BANKING?

🟩 Business risk: open banking requires my business to take ownership of and responsibility for large levels of personal and financial data, which is costly to store and protect, with large financial penalties should anything go wrong

🟦 Customer risk: this is a new service customers are unfamiliar with and its unlikely they will want to share the necessary amount of data

🟥 None of the above



Understandably, the perceived data security risks associated with open banking technology are creating barriers to adoption for businesses and in turn, consumers. However, open banking goes above and beyond to protect the security of businesses and consumers, more so than traditional methods of data transfer and capture, such as screen-scraping.

Specifically, the UK open banking standard is based on a key principle that customers using open banking services will never have to share their online or mobile banking credentials (e.g. username or password) with any third party. Only with the individual's explicit consent will data relevant to the transaction be shared.

The most common model for this process under PSD2 is the redirect or decoupled model, where the consumer's authentication data is exchanged directly between themselves and the ASPSPs (banks and financial institutions). The TPP will not receive the credentials of the user in any way, and after a successful consent process, the TPP can request an access token which can be used for a limited amount of time to fetch data relevant to the transaction from the bank.

The PSD2 Regulatory Technical Standard, which describes the rules and requirements on which PSD2 are based, gives requirements on how these tokens should be securely stored in an encrypted form, protected from unauthorised disclosure and access.

That's why it's a great shame to see 'lack of customer and business willingness to accept risk around data security' is the greatest risk to widespread open banking adoption for over half (51%) of respondents. It's possible that perceived involvement of a TPP in the open banking process is behind this, but all TPPs are subject to the same level of security and licensing regulation as the financial institutions and businesses which use their open banking services.

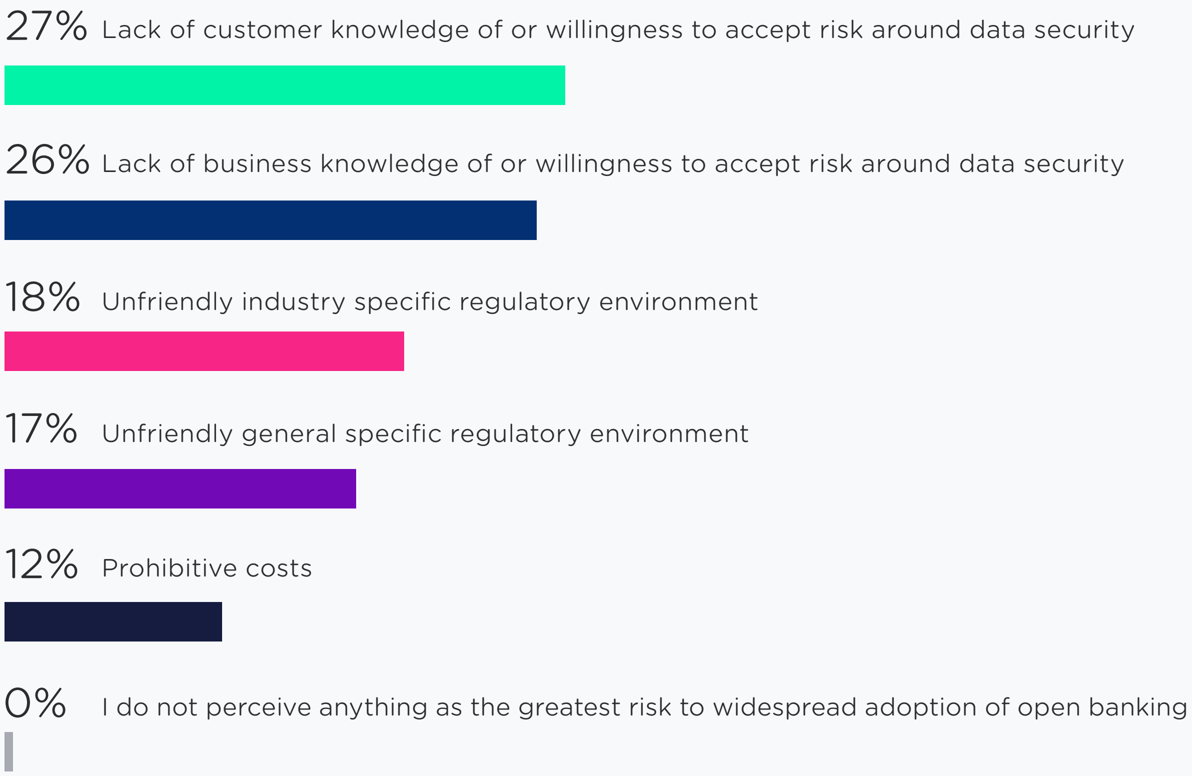
Open banking advocates must help businesses and consumers overcome data security fears, through education, training, and promotion of open banking's inherent security. Most importantly, this must apply to the role that TPPs play in the ecosystem – doing so will help move forward in the path towards increased adoption levels and, ultimately, an open financial system powered by democratised open banking provided by TPPs.

As with any technology, there are of course legitimate concerns regarding data. The issue, however, arises where perceptions of the threat of risks are based on an unfamiliarity with the subject matter. It is the responsibility of businesses utilising open banking to provide sufficient information and assurance required by end-users that open banking technology is secure, and that any personal data is kept both private and safe. Without such communication, it will be incredibly difficult to reach a state of widespread adoption in society. Customers aren't equipped with the knowledge they need to embrace the open banking framework fully and this will only change through greater awareness, which we can achieve with education, support and strong use case examples.

EDUCATION IS KEY

Concerns over the lack of knowledge or willingness to accept the risk around data security among customers and business are further highlighted in the next graph. Over half (52%) of survey respondents perceive this to be the greatest risk to the widespread adoption of open banking.

Q2. WHAT DO YOU PERCEIVE AS THE GREATEST RISK TO WIDESPREAD ADOPTION OF OPEN BANKING?

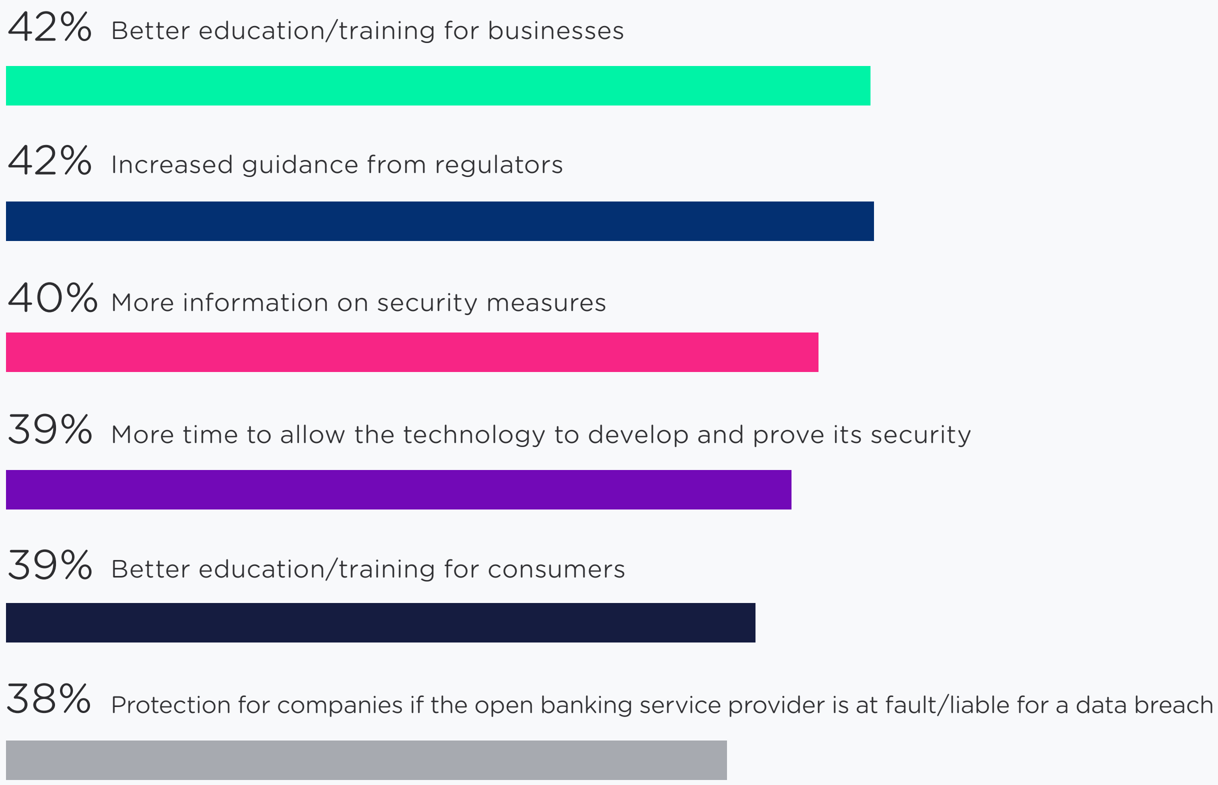


Overall, an unfriendly regulatory environment of some sort was named by 35% of respondents as the third greatest risk to widespread adoption. When questioned further, 22% of respondents from the UK, cited an unfriendly industry-specific regulatory environment, compared to 18% of Dutch respondents who considered the unfriendly general regulatory environment as the third key barrier to widespread adoption.

It is clear that more work needs to be done to foster an environment where businesses fully understand what open banking offers and feel confident in their knowledge of what it achieves, and this responsibility lies primarily with open banking providers, in partnership with regulators. Indeed, better education and support, coupled with guidance on how the data is safeguarded and stored, both with regulators and other players, could help to improve the regulatory environment by minimising the impact of data security concerns on adoption rates.

While the regulatory environment itself is clearly not a security risk, decision-makers and their understanding of, and subsequent regulation of, issues around data security are important in being able to address the risks. Regulators, and their level of appetite for fast-paced change, have not always been in line with the wider industry, but by better educating customers around data security and the measures taken to protect customer data, such as encryption, could lead to both an improved regulatory environment and improved adoption rates.

Q3. WHICH OF THE FOLLOWING DO YOU THINK WOULD BEST HELP TO REDUCE BUSINESS FEARS AROUND DATA SECURITY RISKS?



More information on security measures (40%), both in terms of obtaining and handling the data, is also believed to be important, particularly as it would help businesses understand that open banking is built on highly secure technology, with APIs acting as the invisible plumbing that helps to transmit data securely and enable most online interactions. This would also enable businesses to better communicate this information on security measures to their prospective customers.

Open banking APIs enable banking customers to give permission for regulated TPPs such as Yolt, Moneybox, and Plum, to securely access their financial information. Often, this can unlock better, more personalised products and services – for example, alternative sources of credit, cheaper utility bills, or better savings account options. It's an attractive offering in a post-Covid-19 world.

It is important that customers understand that open banking is based entirely on consent, the customer is in complete control of their data and who they share it with. One concern is around the possibility of unauthorised data sharing or payments, but there is always a consent or authorisation step before any connection and transfer of data occurs between their bank and a registered TPP.

Building on this knowledge and instilling trust in consumers is vital to increasing open banking adoption. Organisations such as the Open Banking Implementation Entity (OBIE) have worked hard to achieve this, with its key objectives being to source opportunities to help improve consumer trust in open banking. These include options to improve management of customer consent, enhanced signposting for customer complaints and redress, and improved security and fraud good practice guidance for third party providers. OBIE also regularly reviews and shares good practice with all open banking participants and has established working groups to support cross-ecosystem collaboration on security and fraud.

Educating customers and highlighting these measures requires collaboration with similarly aligned industry bodies, such as regulators like the Financial Conduct Authority and European Banking Authority and would help to further promote customer confidence and trust in the open banking framework.

INTERVIEW WITH BRONWYN BOYLE, OBIE

YTS sat down with Bronwyn Boyle, Head of Security & Counter-Fraud at the Open Banking Implementation Entity (OBIE) to discuss our research findings and get her thoughts on how to approach education, training, and building trust to unlock open banking's full potential.

Do you agree that better education and training for businesses and increased guidance from regulators are the key tactics which will allay business fears about open banking?

Absolutely. The main barrier to uptake that I see is a lack of familiarity about how open banking works. Open banking is all about increasing competition and innovation in financial services – the industry and regulators have to work together to provide the support and education businesses need on both technical elements and benefits.

Businesses also have to understand that open banking is built on highly secure technology. APIs are the secure, invisible plumbing that help transmit data securely and enable so much of our online interactions. They unlock better, more personalised products and services, and the customer owns their data and is in complete control of authorising any connection between their bank and a regulated third party.

What can regulators do to begin addressing the knowledge gap?

In the UK we can use the lessons learnt from establishing the open banking framework as part of our transition to open finance, and regulators are doing great work to support organisations in their open banking journeys. At the OBIE we've fostered a strong collaborative relationship with the FCA and ICO, working together to improve customer trust and user experience and providing guidance and support to participant organisations.

It will be interesting to see how regulators work together to clearly define tighter requirements for access to and sharing of data beyond PSD2, as not all account types are covered by the controls mandated for open banking. It will also be crucial for regulators to encourage the provision of additional customer information, especially in relation to what recourse customers have if data is misused.

How important is building consumer trust in the work to drive open banking adoption?

It's essential; in fact, it's one of the key OBIE Roadmap objectives. Things like improving management of customer consent, enhancing signposting for customer complaints and redress, and improving security and fraud good practice guidance for TPPs. Understanding customer preferences and behaviours is also key.

To what extent do you think concerns over data security have hindered open banking? Why do you think they have arisen?

Some banks and third parties initially struggled to meet the stringent security requirements of the standards and that slowed down the initial uptake of open banking by end customers.

There are also concerns in regard to Authorised Push Payment (APP) scams targeted at online and mobile payments. If anything, open banking should help reduce the occurrence of such scams, given it introduces another authorised party (e.g. a Payment Initiation Service Provider or PISP) into the chain. There have also been some worries about the sharing and use of open banking data outside of the PSD2 perimeter, but this is largely addressed by existing GDPR regulations.

Overall, the continued adoption of open banking services by end customers is testament to the strength of the current standards and security model. We're looking forward to seeing adoption increase as customers and businesses alike become more familiar with how open banking works and the advantages it brings.

UK vs NETHERLANDS

Koen Mol,
Senior Consultant, Yellowtail

To identify whether the barriers to widespread adoption of open banking are the same across the board, YTS' research examined data security in the context of the UK and Dutch markets, both of which are at different stages of open banking development.

Although historically the UK has been slightly ahead of its European counterparts in the rollout and adoption of open banking, things are beginning to level out and the Netherlands is starting to gain ground as more businesses adopt the open banking framework. Interestingly, while the research found that better education and training for businesses and increased guidance from regulators were considered fundamental drivers for the greater adoption of open banking in both markets, the importance given to each varies between the two countries.

Survey respondents in the Netherlands cited increased guidance from regulators (42%) as being just as important as better education and training for business (41%) in helping to reduce business fear around data security risks. There was a slight difference for 44% of UK respondents who believed the priority for reducing business fears is to focus on better education and training, followed closely by increased guidance from regulators (42%).

The biggest difference between the two countries was that educating and training consumers on the workings of open banking was considered important by 41% of respondents from the Netherlands in addressing business fears around security risk, with 37% of UK respondents feeling the same. Even if this difference is fairly small in practice, it highlights the fine but important line between overall attitudes and different implementation approaches and regulatory enforcement on the ground in the different markets. These approaches will have a material impact on the continued adoption of open banking, but we can't overestimate the importance of underpinning attitudes.

The findings are reflective of the challenges Dutch operators face around consumer adoption of open banking, as many people are concerned about what open banking means for the security of their personal data. There has been extensive focus on GDPR and the importance of protecting data over the last two decades, so this move towards open banking means customers need to be re-educated about sharing data more freely within open banking framework.

Differences were also seen in who or what poses the greatest threat to data security with open banking, with scammers cited as the number one threat by 41% of respondents in the Netherlands. In contrast, increased cybercrime (38%) was the main concern among UK respondents, with scammers (35%) third in line after technology failures (36%), with the latter perhaps a reflection on the intense scrutiny UK banks have endured from regulators on the subject of operational resilience in the financial services sector following a number of IT outages late last year.

Lack of customer knowledge or willingness to accept risk around data security was perceived as the greatest risk to widespread adoption of open banking by 29% of Dutch respondents compared to 24% of UK respondents. In contrast, 25% of UK respondents believe lack of business knowledge of, or willingness, to accept risk around data security was the greatest risk, along with 26% of Dutch respondents.

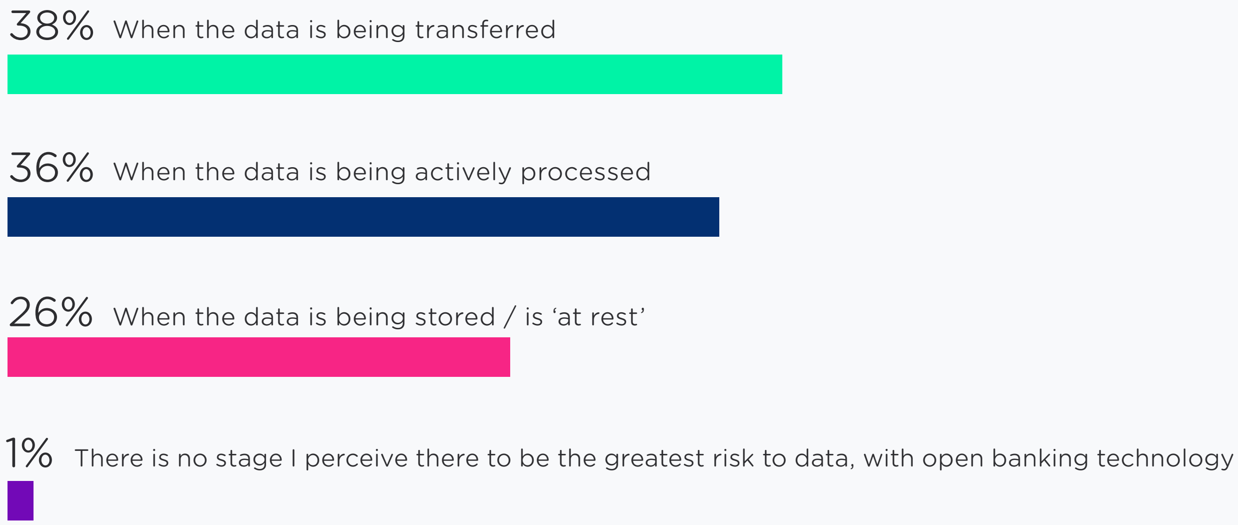
Regionally, these findings show that in the Netherlands more emphasis is placed on the need for consumers to be educated on the workings of open banking if the framework is to be wholly embraced, while answers from UK respondents suggest more work needs to be done to educate those businesses adopting the technology if greater adoption is to be achieved.

SAFEGUARDING CLIENT DATA IS AN INTEGRAL PART OF OPEN BANKING

– Roderick Simons, Chief Technology Officer, YTS

While there are always legitimate concerns surrounding the risks to providing access to accounts and data, it is important to acknowledge that security has always been at the heart of the open banking framework. Open banking was created in order to address security concerns by developing a standard that enables people to access payment data in a structured and secure way.

Q4. AT WHICH STAGE DO YOU PERCEIVE THERE TO BE THE GREATEST RISK TO DATA, WITH OPEN BANKING TECHNOLOGY?

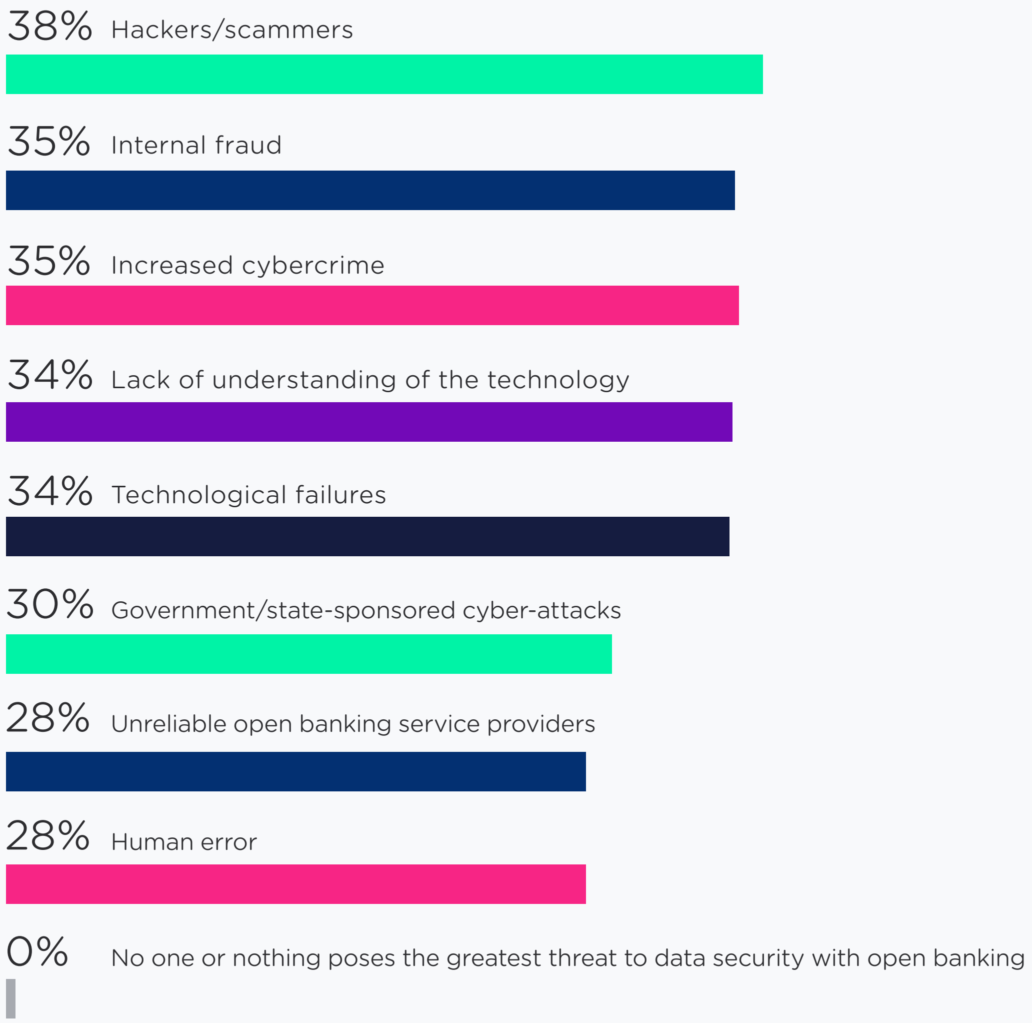


Providers have a duty to ensure that data is kept safe from the first moment they access a customer’s details, so security is an ongoing process, not a momentary one.

When data is being transferred, the PSD2 RTS states that encryption must be applied between the parties throughout the respective session in order to safeguard the confidentiality and the integrity of the information. The UK open banking regulation specifies this in more detail, where mutual TLS (Transaction Layer Security) and the minimum supported algorithms are prescribed.

Furthermore, under PSD2 the processing of sensitive data must take place in secure environments in accordance with strong and widely recognised industry standards.

Q5. WHO OR WHAT POSES THE GREATEST THREAT TO DATA SECURITY WITH OPEN BANKING?



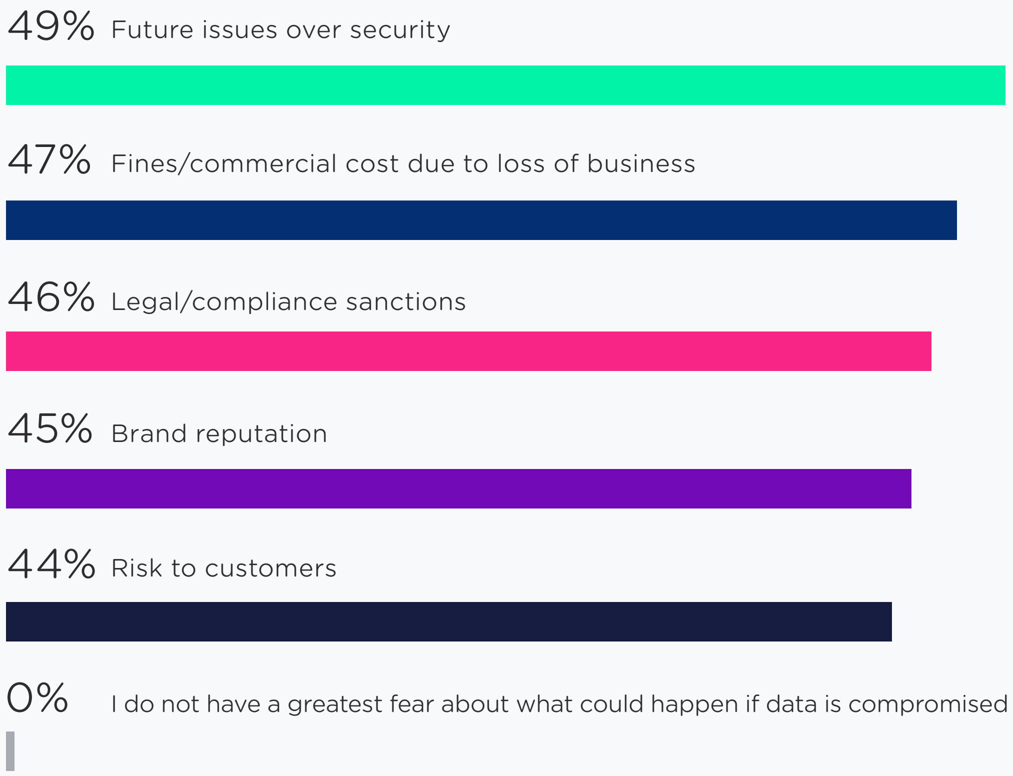
Despite this, the research shows that threats to data security remain front of mind for many of the survey respondents, with hackers (38%), internal fraud (35%) and increased cybercrime (35%) cited as the top three concerns. Technological failures (34%), government/state sponsored cyber-attacks (30%) and human error (28%) are also listed as key worries.

Interestingly, internal fraud (38%) was considered the second greatest threat among Dutch respondents, with technological failures the fourth greatest fear. In contrast, internal fraud was only cited by 32% of UK respondents, ranking it fifth in line of risks to data security. This may be due to the perceived strength of internal fraud prevention measures in each country's open banking systems.

Overall, 28% of survey respondents cited unreliable open banking service providers as one of the greatest threats to data security with open banking. This is perhaps largely due to unfamiliarity with the licensing requirements TPPs have to pass, and is one of the most dangerous misconceptions around the role of service providers and something which could be significantly holding back adoption. All TPPs are subject to stringent regulation covering data handling and storage, and are a secure part of the whole open banking ecosystem.

This message needs to be communicated to all businesses more clearly across the open banking map to enable TPPs to spread open banking to all who are considering adopting the technology, including how their users' data is handled, stored, and kept safe. That job rests not just with the providers themselves, but also with the regulators which oversee the financial systems, providing official, clear, and accessible guidance for any firm which needs either education or reassurance.

Q6. WHAT IS YOUR GREATEST FEAR ABOUT WHAT COULD HAPPEN IF DATA IS COMPROMISED?



Respondents also outlined their greatest fears about what could happen if data is compromised, with future security issues top of mind (49%), particularly the resultant fallout this could have on the business, followed by fines and commercial cost due to loss of business (47%) and legal/compliance sanctions (46%). Damage to brand reputation was a concern for 45% of survey respondents while the risk to customers was ranked a key risk by 44% of those surveyed.

But with scammers becoming more sophisticated, relying on legacy banking technology may no longer be enough in the coming years. Instead, investing in API technology with greater transparency about data handling and storage can not only protect customer's data but also improve brand reputation, gaining a competitive edge at a crucial economic time.

And if something ever did go wrong, PSD2 dictates that responsibility lies with the licensed and regulated parties that are involved in service provision, within their own domain. For example, if there was a fraudulent payment, the financial institution would reimburse the money and the TPP must provide a thorough investigation into the circumstances behind the problem. Crucially, both consumers and businesses are protected by strict and stringent regulatory procedures in the event that there is a breach.

There is also the clear issue of brand reputation in an event such as this – if a breach or failure were to happen, it is an understandable concern that public image could be damaged. That's why it's vital that regulators are clear about best practice to prevent a breach, and their relationship with and licensing of TPPs. This is especially the case with open banking as it is a new and transformative technology, so guidance which covers external regulation and internal processes needs to be as clear and accessible as possible.

The findings illustrate a clear need for customers to be better educated around the workings of the open banking system. Regulations such as PSD2/RTS include several crucial controls that significantly reduce the risks cited and we need to educate customers about the fact that the open banking ecosystem is secure and cannot be accessed by just anyone.

Fintechs and new service providers must undergo stringent requirements to demonstrate they have robust security and risk management controls in place before they are authorised by regulators to participate in the system. They are also continuously overseen by the regulator to ensure standards are maintained.

Highlighting this message and educating customers of the rigorous processes involved could go some way to addressing what some might claim to be unfounded claims against the perception of "unreliable open banking service providers." This responsibility should sit with the entire open banking ecosystem – from TPPs ensuring that businesses understand the secure design on which open banking was built, to regulators giving clear and accessible guidance to the firms under its jurisdiction. Availability and clarity of information is crucial, but that alone isn't enough – if the goal of open finance is to be achieved, the message must be spread proactively, far and wide.

PRODUCTS AND SERVICES ARE ALREADY BENEFITING FROM OPEN BANKING

– Koen Mol, Senior Consultant, Yellowtail

While there is certainly a knowledge gap among SMEs and consumers on the benefits of the open banking framework, one of the main challenges facing widespread adoption of open banking is that as an "under the bonnet" technology, there is no real reason why customers should be aware of it, even if it transforms the way they manage their finances.

However, what consumers and businesses do need to know is that the products and services that open banking enables represent a new wave in financial services. Similarly, it is important for businesses to help customers realise that a broad range of products and services tailored to support the complex needs of banking customers and businesses has already been developed and is available to them. The ongoing development of open finance and highlight its potential could also attract new customers to embrace open banking; open finance isn't a 'niche' offering, it has the potential to change the way we look at our finances.

Products such as flexible loan applications and real-time cashflow management, accounting software and debt advice are open-banking-enabled products designed to meet evolving customer needs. This is particularly relevant currently, when many customers are under increasing financial pressure owing to the COVID-19 crisis.

Although the COVID-19 outbreak and subsequent lockdowns in the UK and the Netherlands have undoubtedly disrupted some existing open banking projects, the financial services industry has responded well to the crisis. In fact, 12% of financial services companies survey in our 'Unlock the Value of Open Banking' report said the COVID-19 crisis actually accelerated their plans to adopt open banking technology.

As well as this, behind the scenes, products have been adapted and services have been tailored to tackle the urgent needs of consumers and SMEs feeling the effects of the massive disruption to the economy and subsequent challenges of how to recover or even survive the fallout.

We need to see a bigger and positive push to get this information out to all stakeholders in the financial ecosystem – not just the businesses who are looking at adopting technology, but also their partners and crucially the customers who will benefit day-to-day.

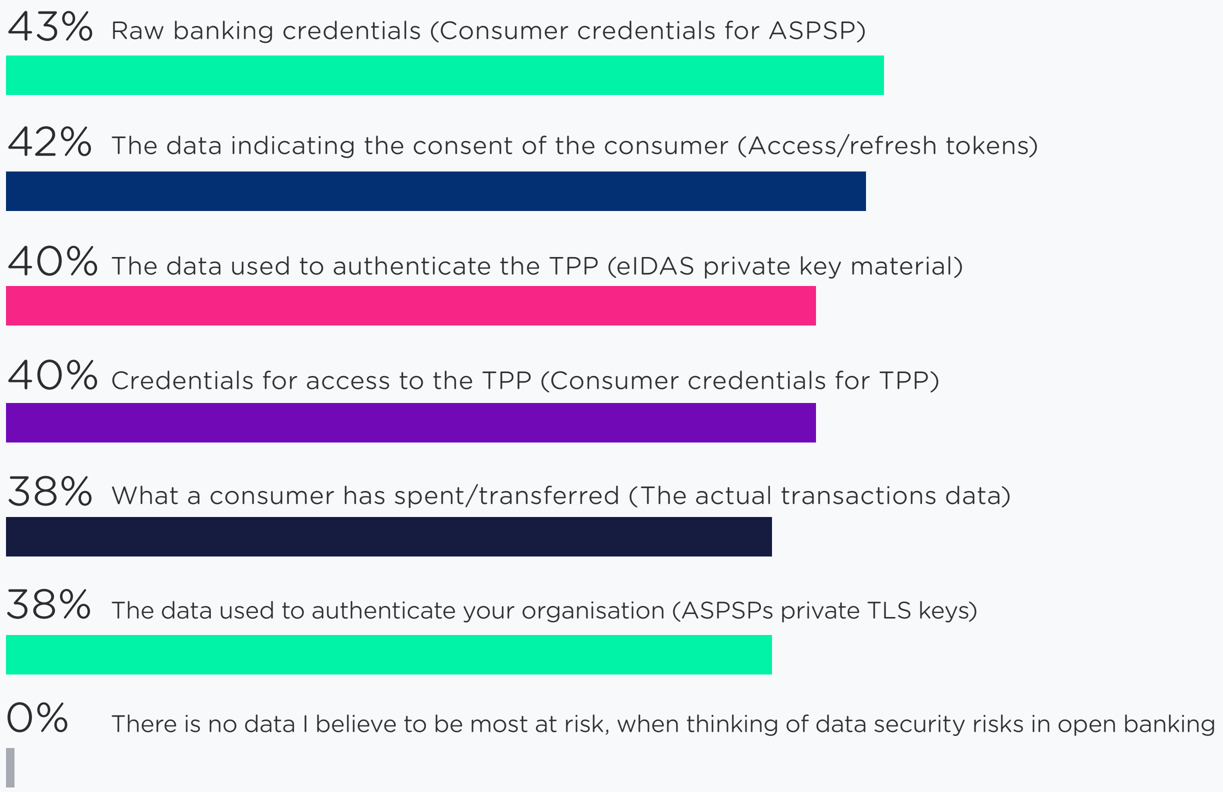
WHICH SPECIFIC DATA CONCERNS DO RESPONDENTS HAVE?

– Roderick Simons, Chief Technology Officer, YTS

While many different concerns over data security risks are common with all aspects of technology, our research shows that risks to raw banking credentials (43%), data indicating the consent of the consumer (42%) and the data used to authenticate the TPP (40%) were the top three threats highlighted by survey respondents. It's worth noting here that no credentials are shared with open banking, so this particular finding is the result of a misconception around the process.

Concerns relating to consumer credentials for access to the TPP (40%), details of consumer transaction data (38%) and the ASPSPs private TLS key (38%) were also listed as security risks. This data reveals the greatest level of consistency across the survey, with all possible concerns within 5%. This presents a wide but equal perception of the threat landscape.

Q7. WHEN THINKING OF DATA SECURITY RISKS IN OPEN BANKING, WHICH DATA DO YOU BELIEVE TO BE MOST AT RISK?



It is important to note that these concerns are addressed by the fact that open banking mandates that Strong Customer Authentication (SCA) is implemented to ensure the security of online payments and access to accounts, and that secure encryption is applied for the storage of the most sensitive materials like consent records. SCA requires multi-factor authentication to verify the customer's identity, making it more difficult to compromise authentication credentials. Customers sign in with their bank, so the open banking transaction uses the actual bank's security, which customers already trust.

Furthermore, rather than relying on each individual bank to validate the identity of an ecosystem participant, open banking is based on a standardised trust framework, which involves the issuing of trusted digital certificates that banks can rely on to automate the identification and validation of participants' identities and their regulatory permissions. This not only reduces the chance of fraud, but it also speeds up the transactional process.

Similarly, OBIE and the OpenID Foundation (OIDF) have worked together to define a security profile (the FAPI profile) which provides a secured standard for the sharing of sensitive payment data. In addition, OBIE also regularly reviews and shares good practice with all open banking participants and has established working groups to support cross-ecosystem collaboration on security and fraud. For example, OBIE has recently partnered with IASME to develop a counter-fraud certification scheme to help organisations ensure they have the right controls in place to combat fraud.

However, concerns clearly remain and there is a great opportunity to educate businesses that haven't yet embraced open banking on these concepts and ensure they understand how the ecosystem operates and how risks can be reduced. It is only through education that these concerns can be alleviated, and the adoption of open banking will continue to grow, something which is of more importance than ever given the economic and societal disruption caused by the COVID-19 pandemic. That needs to be proactive and inclusive, with opportunity for businesses to express their concerns and be provided with resources and information to allay them.

YTS CALLS FOR THE CREATION OF A NURTURING ENVIRONMENT FOR INNOVATIVE FINANCIAL SERVICES

– Roderick Simons, Chief Technology Officer, YTS

Despite encountering some early resistance from within the financial services industry, open banking has evolved substantially since the Competition and Markets Authority first issued its mandate to bring more competition and innovation to the sector.

While the move to open banking hasn't always been straightforward, there are millions of active open banking users and the market has continued to grow through a combination of great results and participant's commercial marketing efforts.

Although the number of open banking users is close to reaching the three million milestone in the UK, there is still a great deal of work to be done if the true potential of open banking is to be fully realised. Fostering the right environment for open banking to develop is imperative to its evolution into open finance, and we believe that currently there is not enough incentive for established firms to move towards open finance.

To create the nurturing environment which will enable this transition, concerns and issues first need to be addressed, and it is clear that data security is one of them. Open banking has high-grade safeguards and any data stored is encrypted with_advanced and intricate security measures. GDPR requirements add a further level of security so customers can be assured that multiple measures are in place to protect their data.

The fact is, open banking was designed to provide greater security for customers by giving them ownership of their data. It also opens up a wealth of products and services that would not have been available without the open banking-enabled framework. Customers need to know this, and it is the duty of the regulators and the industry to work together to provide the support and education businesses and consumers need, not only to understand what open banking is, but how it can directly benefit them.

In particular, businesses would appreciate more formal education about the benefits that open banking can provide for SMEs and consumers and the robust measures that have been put in place to guarantee data privacy. Advocates of open banking, from regulatory players to open banking providers should drive this educational campaign amongst businesses, otherwise adoption progress may suffer if the whole industry isn't behind it.

This is not the only barrier which needs to be broken down, but doing so will lead to progress in other areas of the open banking ecosystem.

A current barrier for a business to access customer data is that there are no commercial or regulatory incentives for banks to make their APIs available, and no API performance is benchmarked against a minimum standard, or regulated if performance drops. Once this is solved, the next big issue already on the agenda is lack of data uniformity, where without clear guidelines, the sheer amount of different data formats and fields could deter easy access to data. This could be an obstacle in the move towards open finance as the data received from banks is mixed. From an open banking perspective uniformity is there, but it is up to the bank to interpret this in their own way and a lot of data fields are optional to provide.

Introducing data uniformity into the market could be a huge opportunity. Today, every ASPSP - any financial institution that offers a payment account with online access - provides different data fields, and for a lot of ASPSPs the same data field has a different definition. The lack of some clear, aligned and uniform data fields, such as account holder name, currently do not allow the industry to effectively fight fraud during KYC checks, for example, though there are signs this is changing with the OBIE's recent payee field standard requirement. Next to this, due to the absence of fields in one ASPSP versus another, services based on their APIs cannot be uniform towards consumers.

Ease of use for the consumer is critical in the success of open banking. If the consent journeys for consumers are too complicated (e.g. downloading a separate MFA token app which requires additional credentials to authenticate their identity) they will not participate. More focus and alignment on easy-to-use consent journeys through mobile banking apps, and the fingerprint and facial ID systems they use, would greatly benefit consumer adoption by addressing security concerns.

MOVING TO AN OPEN FINANCIAL FUTURE

There is a great opportunity to use the lessons learnt from establishing the open banking framework as part of our transition to open finance. A set of rules and guidelines, like with open banking, would encourage the move towards open finance and clear data sharing guidelines should be put in place for SMEs as GDPR currently only covers individual consumers.

There needs to be a fair representation from all ecosystem participants to ensure that the outcomes are satisfactory for all and eventually benefit the consumer. In addition, the FCA has an important role in overseeing that firms adhere to the new rules and collaborate in the ecosystem.

It's clear that the open banking framework has the potential for much broader benefits, and the UK government has stressed that it views open finance as the right and natural next step in its evolution. The current model is limited in scope and, while it makes sense for the open banking model to be expanded in other financial areas, there is still a lot of work to do before this can be achieved.

Adoption of open banking has only just scratched the surface. In order to improve take up rates, more must be done to explore new methods and mechanisms that promote customer confidence and trust in open banking. This can be achieved through better education and support around how data is stored and the measures in place to safeguard client data.

This in turn should help to foster a more open and collaborative regulatory environment that is nurturing and informative. It will also encourage greater adoption among providers by addressing some of the misconceptions surrounding the framework that act as a barrier to take up.

Finally, establishing a uniform set of data fields and common and agreed standards that can be provided by firms and alignment in the consumer consent journey is also crucial, and both regulators and industry bodies need to work together to achieve this common goal.

It is through industry and regulatory collaboration and greater education that the barriers to open banking adoption can be addressed and the model can truly realise its full potential. This is happening in places, with amazing results achieved so far, but we're just at the start of this journey. Changing the future of the financial system is a priority for YTS, and we want to see that commitment shared by more throughout our sector and beyond. We are on the right track, and the future is bright – we just need to keep walking towards it.

END

CONTRIBUTORS

RODERICK SIMONS

Chief Technology Officer, YTS

Roderick is Chief Technology Officer (CTO) at Yolt: the smart thinking money app empowering over 1.6 milion people in the UK, France and Italy to be smart with their money. Roderick also works across the B2B arm of the business, Yolt Technology Services (YTS), which brings the power of open banking to businesses across Europe.
Roderick has been leading innovative technology solutions at Yolt since 2016 as one of the four founders of the Yolt app. Security and safeguarding customer data are core values at Yolt, and a top priority for Roderick. He's responsible for ensuring the strongest possible protection for both app users' data and YTS's client data through rigorous stress testing of bank-level security using physical, electronic and operational measures. Roderick also leads on IT strategy; creatively planning and problem-solving complex company-wide IT solutions.

Roderick started his career building ING's mobile banking app, which is now used by over four million users. Following the success of its launch, he was presented with the opportunity to join Yolt and tasked with building a pan-European smart money app from scratch.

BRONWYN BOY

Head of Security & Counter-Fraud at the Open Banking Implementation Entity (OBIE)

With over twenty years' experience leading and advising international organisations in cybersecurity and technology, Bronwyn Boyle is currently Head of Security & Counter-Fraud at the Open Banking Implementation Entity (OBIE). Open banking is a secure way for customers to take control of their financial data and share it with organisations other than their banks, opening up better value and choice. With a background spanning technology development, cyber security, compliance, data protection, strategy and operations, she has as passion for security culture, innovation and improving industry alignment to counter security and fraud-related threats. She also advises a number of FinTechs and RegTechs on security and privacy requirements, strategy and product development.

KOEN MOL

Senior Consultant, Yellowtail

Koen Mol is Senior Consultant at Yellowtail, a Dutch fintech agency, and Technology Lead within Yellowtail Beyond. Beyond uses PSD2 data to facilitate new financial opportunities for customers and better protect them against upcoming events, all to create financial fairness. To achieve this, Koen combines knowledge from clients, technology, data science, design, and legislation. He has experience in the Dutch Mortgage, Consumer Credit and Pension markets.

YTS

Yolt
Technology
Services

```
curl - X POST httpås://api.sandbox.yts.io/v1/users
-- cert tls-certification.pem\
-- key tls-private-key.pem\
-- header “Content-Type: application/jtpsd” \
```

```
openssl req - out tls-csr.pem -new -newkey rsa:4096 -nodes -keyout tls-private-
```

```
REQUEST_TOKEN=$(step crypto jwt sign--iss $CLIENT_ID \
 -- kid $REQUEST_TOKEN_PUBLIC_KEY_ID \
 -- key private-key.pem \
 -- alg RS512 \
 -- jti= ‘uuidgen’ \
 -- subtle)
 echo $REQUEST_TOKEN
```

Contact us to set up a meeting, and let’s explore how we can help your business reach new heights.

w: yts.yolt.com | e: yts@yolt.com

Hoogoorddreef 60
1102 CT Amsterdam
The Netherlands

8-10 Moorgate
London EC2R 6DA
United Kingdom