CLOUDENTITY

The Business Benefits of Dynamic Authorization for Open Banking APIs

CLOUDENTITY

An Introduction

Welcome

APIs are a hot topic in finance today, driven by the rapid adoption of Open Banking, partner ecosystems and digital transformation. The revolution started when regulation changes in Europe were formed to enable innovation in the fintech arena and protect customer privacy.

Since a small cache of banks held the majority of data from the majority of customers, it was difficult for innovative new service providers to break into the market. In the USA, Financial Data Exchange (FDX) has built a consortium of providers around a common standard for secure and convenient access to financial data as well. Now, with the increased ability for customers to share their banking data with any trusted provider in the FDX or Open Banking network, **the chance for smaller financial companies to offer competitive services has skyrocketed.**

It has also presented a gold rush for app developers working to build what will become the new, go-to Open Banking platforms. However, with great opportunities come great risks. The good news is that well-built APIs will mitigate the biggest problems.

Get ready for the Open Banking revolution, get in touch with Cloudentity today.

info@cloudentity.com
(206) 483-2255

1.0

Why are APIs and Dynamic Authorization so important to **Open Banking?**

In short, Open Banking is a system where people's personal and business data can be shared, at their request, to allow easier access to financial products that will save money, time and hassle. APIs (Application Programming Interfaces) are what allow all that data to flow between apps, platforms and financial providers in safe, secure ways.

APIs then help aggregate all the information and present it in a user experience that is easy to navigate. For example, imagine an 'Expedia of finance' that collates all of the best loan deals instead of flights from around the web. Depending on the functions of this Open Banking platform, you'll be able to view all of your money in the different places you have it, move that money around at will, make payments, and also find deals on loans, term deposits, lines of credit and more - all in one spot.

The big challenge is that the security of this information is much more sensitive than Expedia's flight details. The face of online security is fast changing too. No longer are the acl or role-based authorizations of yesteryear secure enough to stand up to the needs of Open Banking. Rather, we need to instantly know the full context of who is wanting access granted to the data. Who are they? Where are they from? When are they wanting access? Why are they needing access? What kind of device are they operating from? That context changes everything.

Dynamically updating Authorization based on that context allows security to correspond to the transaction within the regulatory mandates. For example is it a high value transaction that transfers money out of your account or a lower value transaction such as changing your time zone. Businesses need security that understands the context of every single transaction, in real-time without hampering the customer experience. Because APIs are the gatekeepers of this data, their security is key. Being able to share your data in a safe, reliable way like this will require fully context-aware, Dynamic Authorization and consent for each API the Open Banking platforms are using.

This is harder than it sounds, but is essential to improve the customer experience and customer consent of data sharing within the Open Banking ecosystem.

2.0

What Are The Risks of Open APIs and **Open Banking?**

> The two major risks of Open Banking and Open APIs are authorization based: SECURITY and TRUST. Different standards and organizations have provided baselines for priority but most importantly it's also critical for the customer to choose.

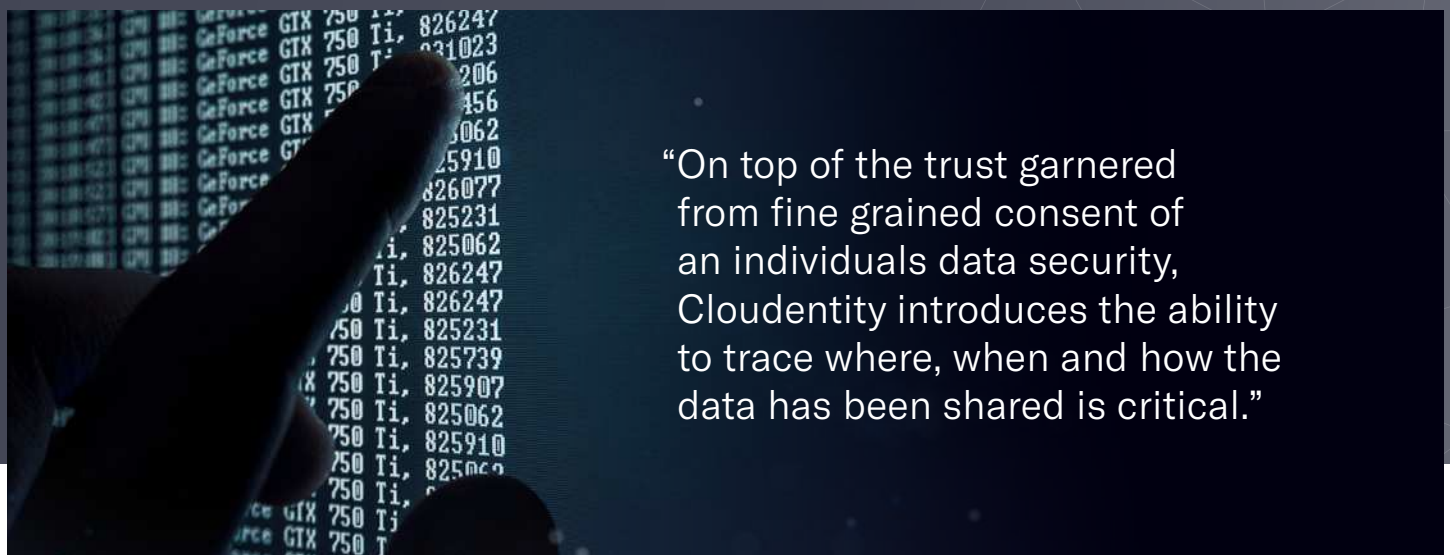
Authorization: Security

It goes without saying that when people or businesses share their financial details, they want it done in a secure way. The opportunity for theft, fraud, or unwanted exposure all carry extremely high consequences. If an Open Banking API doesn't have proper identity and authorization in place, then criminals could transfer all of your funds from your accounts or take out loans or credit cards in your name and rack up millions in debt. More subtly, if an advertiser gets a hold of your transaction details, they could manipulate your future purchases through targeted marketing. If a competitor has access to all of your banking data they could much more easily undercut your prices, or target your existing customers to take business away from you.

In addition, it's important for consumers to provide intent and direction on how their data is being used. Some customers may only want their name shared and not the rest of their user profile. Other customers may only want to share transactional data one time or for a week. All of this context adds to the risk profile managed at the authorization level. Since all of this data is flowing through Open Banking APIs, it's critical for authorization to become context-aware: dynamic and to take place within the API itself.

Thus, for Open Banking to be successful, it needs to use APIs which share data in a way that is secure. Users also need to be able to only share their data when they want it shared, with who they want it shared with, and only for the time they want it available.

That brings it to the next big risk; trust. →



> "On top of the trust garnered from fine grained consent of an individuals data security, Cloudentity introduces the ability to trace where, when and how the data has been shared is critical."

Authorization: Trust

For the Open Banking system to work, any provider that is allowed to participate must be trustworthy. In places like the UK and Australia there is strict legislation that requires Third Party Providers to go through an authentication process with their respective competition and consumer governing body before they can participate. This is to ensure only legitimate businesses with their client's best interests at heart have access to the financial data people are willing to share. First and foremost, these regulations help ensure security and reduce the risk of bad actors manipulating the system for selfish or criminal interests. What regulation makers also realize is that if users don't trust that the system is secure, and that suppliers will responsibly use data to offer products which will benefit the user, then people simply won't use the system. Then everybody loses.

As a first step to build trust, Third Party Providers must use secure APIs with dynamic, fine-grained authorization that will respect the consent of users and keep that data safe. Those APIs need to assess the context of any Third Party seeking authorization in real time, otherwise it will hamper the user experience and leave people frustrated. More importantly, if there's just one security leak it will undermine trust in the system. That means if a supplier is seen to be negligent in their security or treatment of Users consent they'll essentially either ruin the reputation of Open Banking or lose their customers and be ejected from the Open Banking ecosystem. However, if, for example, a Third Party Provider like a chartered accountant can prove they're using a secure platform with secure APIs that use context-aware, Dynamic Authorization, then they can cement a foundation of trust at the ground level.

On top of the trust garnered from fine grained consent of an individuals data security, Cloudentity introduces the ability to trace where, when and how the data has been shared is critical. This is called Data Lineage and adds transparency to the process. Data Lineage also ensures if something goes wrong, then issues can be resolved with the appropriate parties. Adding this capability into the system adds an extra layer of confidence that if problems arise, they'll be sorted out quickly and satisfactorily.

Finally, users need to trust that Third Party Providers who receive their financial information will use it to benefit that individual or business

By offering better products, better prices, better convenience and better customer service, increased trust will be fostered with certain Financial Providers over others. If everyone does this in good faith, the entire system and all users benefit. As they say, a rising tide floats all boats.

So, how do you ensure you have Dynamic Authorization that protects these Open APIs?

3.0

How to Mitigate Security and Trust Risks in **Open Banking?**

As mentioned, well-built Open Banking APIs will be critical to exchanging data and Dynamic Authorization will ensure the security of Open Banking data, help foster trust in the system, and streamline the usability of the system. Cloudentity's Authorization platform provides fully context-aware, Dynamic Authorization and fine-grained trust based consent that goes well beyond traditional models based on roles or lists.

Old hard-coded security models can no longer protect you in Open Banking's high risk world, with multiple points of potential security failure. Instead, Dynamic Authorization, links to your applications, data, or other sensitive assets, then grants or denies access in real-time by policy, according to the context of the Five W's (who, what, where, when, and why) of the user and transaction. This context generates a full risk profile for the transaction and grants authorization only if theres a policy based match. The possibilities here are endless.

For example, context for one transaction might look at a Thirty Party and ask what kind of authentication type they're using, what the proposed value of the transaction is and whether that sits within limits set by the user, where in the world they're seeking access from, what time the transaction is happening, whether it's from a known mobile or desktop and whether the users behavioral patterns and fraud engines match the expected model and privacy regulations for the country the user is in. Every jurisdiction is different. Every authorization is different too. Context changes everything.

The great thing about context is, knowing the ins and outs of every data transaction allows for better authorization and data sharing with Third Party Providers based on users' preferences. This means increased customer satisfaction and loyalty by meeting mutual goals. So, context-aware, Dynamic Authorization not only provides enhanced security for your technology and financial assets, it also transforms your customer's experience from static policies to dynamic fulfillment.

The following are essential solutions any Dynamic API will need to have, to deliver the very best benefits to users and businesses . If what you're using doesn't tick all the boxes, its time to consider switching to something like Cloudentity.

These essential features include:

Common Sharing

Because Open Banking is about sharing data between multiple businesses and their corresponding software platforms and services, having the ability to work across the board universally is mandatory. APIs which use FAPI based OIDC and OAuth 2.0 and 2.1 do this with other benefits built in too. OAuth and OIDC are the authorization protocol that allows you to use your Facebook or Google account to sign into other apps and platforms around the internet. Similarly, you'll be able to use Open Banking authorization to log into multiple banks through a single pocketbook app.

Authorization Server & Consent Enforcement

Cloudentity's OAuth 2.0 and 2.1 based Dynamic Authorization provided to protect APIs also comes with fine-grain data access to ensure that access to APIs take consent and user privacy preferences into account. In short, when a user uses a device or application accesses an API, consent is a factor that is considered when determining access. You can select which Third Party Providers you consent to have access to your data and which ones you don't. This is key when keeping your data in the correct hands and more secure in the long run.

Intelligent Threat Protection

When your platform's Open Banking APIs communicate with another organizations API, you want it to automatically detect risk and threat analysis by analyzing transactional cyber data and third-party reputational data to determine whether a connected device or application is valid or potentially fraudulent. This keeps both the financial data itself and the Open Banking platform safe from hacks in a way that is fast, seamless and always on.

"Customer Consent is the bedrock of building trust with organizations. Open Banking and Open APIs must rigorously support the ability for customers to manage their consent at the data object level."

Step Up Authorization

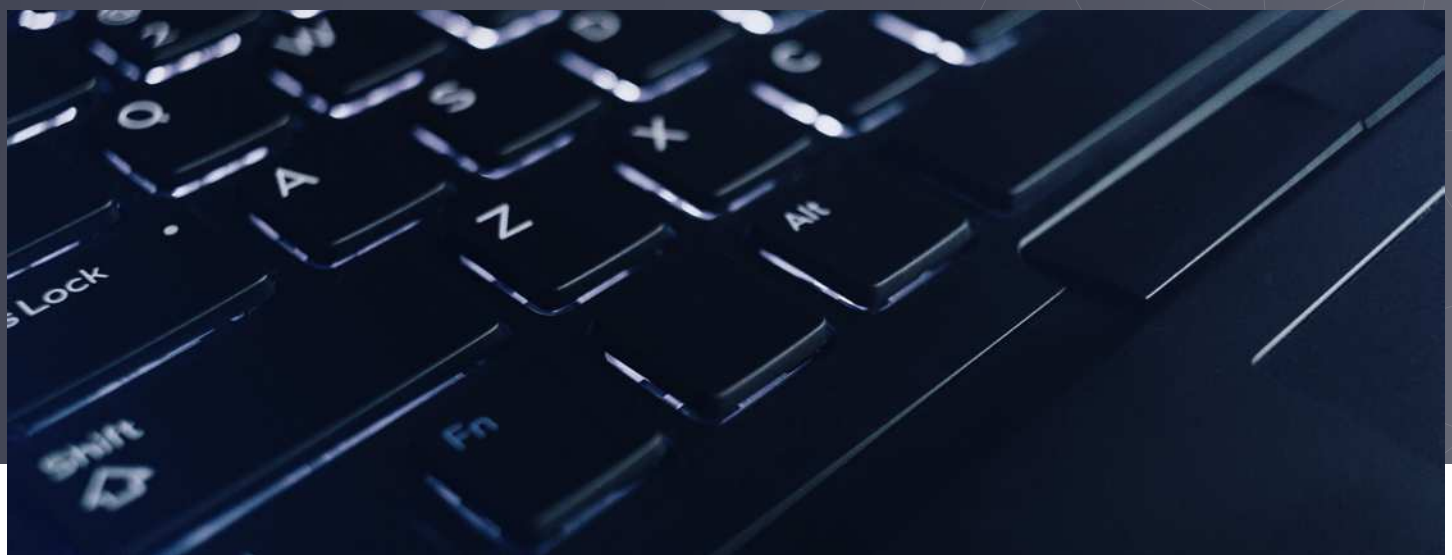
Step up Authorization adds additional security for APIs by enabling an extra layer of authentication like Multifactor Authentication performed on a transactional basis or for ones that appear suspicious. You may also choose to use step up authorization for large transactions over a certain amount, whenever dealing with new Third Parties, or other user scenarios.

An example of step up Authorization might be a one-off password sent to a secure mobile phone or email address, FIDO-based biometric authentication, or an extra pass key generated through an authentication app. This way, valid connections and use cases are allowed through, while bot-traffic and malicious applications are prevented.

Fine-Grained Customer Consent Management

Customer Consent is the bedrock of building trust between a user and an organization. Open Banking APIs must rigorously support the ability for customers to manage their consent at the data object level. Cloudentity provides a singular place for consent management for all APIs and services.

Customers are able to quickly and easily see that their entire user profile is being shared with their main bank, but only their UID (unique identifier) and transaction #7 are shared for a singular usage with a credit review agency. This gives consumers the highest levels of trust that the Open Banking platform is treating their privacy and data with the utmost respect and providing Immutable Audit Logs of how, when, where and why that data was shared.



Immutable Audit Logs

Tamper-proof logs of every transaction, authorization request, consent given and all connected devices, enable security and compliance teams to have the proper documentation to prove compliance with regulations. As mentioned above, knowing that audit logs are available for viewing also builds trust with users who know everything is traceable should any unlikely issues ever occur. It allows for swift resolution of problems, with the responsible parties being pinpointed in the network quickly, efficiently and without mistakes. Cloudentity's privacy ledger (https://docs.authorization.cloudentity.com/info/concepts/privacy/privacy-ledger/) provides Immutable Audit Logs and Kantara consent receipts for all Open Banking and Open APIs giving the highest levels of trust and traceability to end users, banks and third party providers.

Data Lineage

Building trust with customers requires trust. The trust to know an organization will only use your data in the ways, and shared to the third parties, one specifies. The Data Lineage capability of Cloudentity's Authorization fabric adds this much needed traceability. There's a single screen for business and consumers alike to analyze where and how their data has been transmitted down to the individual service level.

Cloudentity Dynamic API Authorization and Governance

Like with any technology, APIs need to be user friendly for those who integrate them into different platforms and systems. It also includes customer and developer portals with built-in, financial-grade authorization and governance. These provide customizable portals, with seamless integration of existing identity providers, to provide developer self-registration, API governance, authorization, documentation, and credential creation. So, not only is it easy to use, it's secure, accountable, and builds trust.

Cloudentity's platform not only includes all of the above essential security and trust features needed for Open Banking, but delivers Dynamic Authorization and Open Banking policy packs to provide security and privacy guardrails for developers; reducing development time for new initiatives by up to 85%.

So, not is it only secure and easy to use, it's easy to update as regulations change and the industry evolves. This is absolutely essential in a fast-moving environment like Open Banking where speed to market for new features and applications is paramount.

Conclusion

Open Banking dramatically changes the way people and businesses manage their money. Like no other development in decades, it puts the power of financial data back in the users' hands to ensure that data can be used for their own benefit.

The benefits of Open Banking are far reaching and multifaceted. From easier access to cheaper loans for businesses, to the ability to manage money quickly and easily, increased competition beyond the big banks, and new opportunities for financial technology companies and startups, the sky's the limit to what this revolution will do.

However, Open Banking is not without its risks. If the financial data isn't property secured by well-built APIs, if sharing consent to Third Parties isn't put in the hands of data owners, if Third Parties misuse the data they are given, then trust in the Open Banking system will crumble.

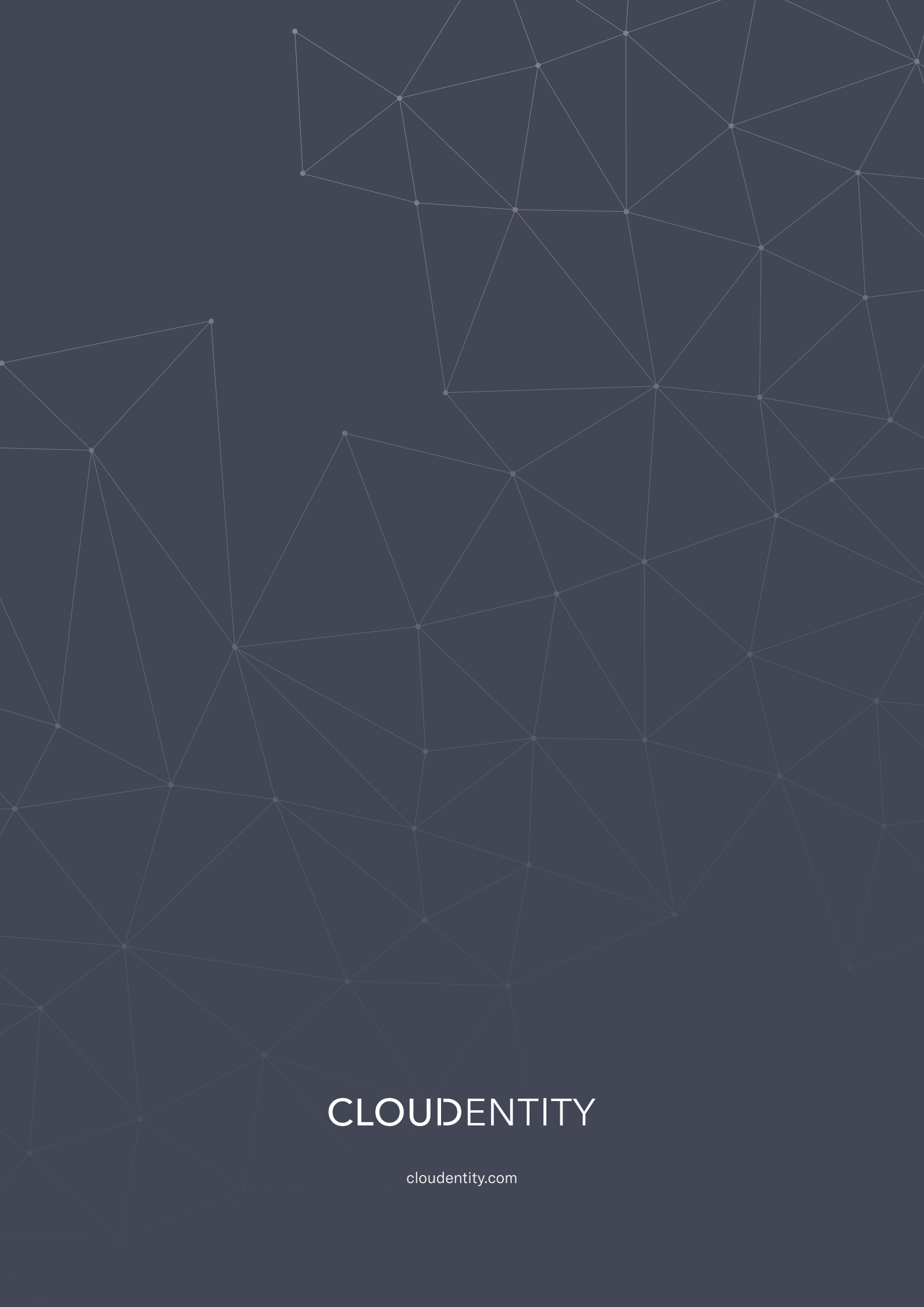
Further, if usability isn't seamless and easy to manage via excellent API portals, with context-aware Dynamic Authorization, the full potential benefits of Open Banking will never be realized. It is essential that good regulation, well-thought out standards, and secure technology are all harnessed to maximize the benefits for everyone . Dynamic Authorization not only solves the security challenges of Open Banking, but also helps assess the context of each data transaction for better protection and usability. This results in the unicorn win/win of better security and better customer experience.

To help, Cloudentity's Authorization Control Plane provides financial-grade APIs along with the management, enforcement and auditing necessary to be ready for Open Banking. It's secure, fosters trust and importantly, helps developers ship projects to market faster. Context changes everything and Cloudentity have just changed the context for Open Banking API standards.

Be ready for the Open Banking revolution, get in touch with Cloudentity today.

2815 2nd Ave, Seattle, WA 9812
info@cloudentity.com
(206) 483-2255

CLOUDENTITY


CLOUDENTITY
cloudentity.com