Columbia Law School
Global Law and Business Seminar: Introduction to Fintech Law

Session #7 July 28, 2022, Morning

Todd H. Baker

Senior Fellow, Richman center for business, Law & Public Policy, Columbia University

Class Outline

- Session #1
  - Introduction to FinTech
- Session #2
  - Fintech Toolkit: The Business Model Canvas, Public Policy, Law & Regulation
- Session #3
  - FinTech Business Models—Consumer & Small Business Lending
- Session #4
  - Fintech Business Models–Alternatives to Payday and Overdraft: Earned/Early Wage Access
- Session #5
  - Fintech Business Models-- Payments Innovation
- Session #6
  - Fintech Business Models– Bank Charters & Fintech Access
- Session #7
  - Open Banking in the US and EU—Approaches and Outcomes
- Session #8
  - The Challenge of Crypto Regulation in US

Agenda

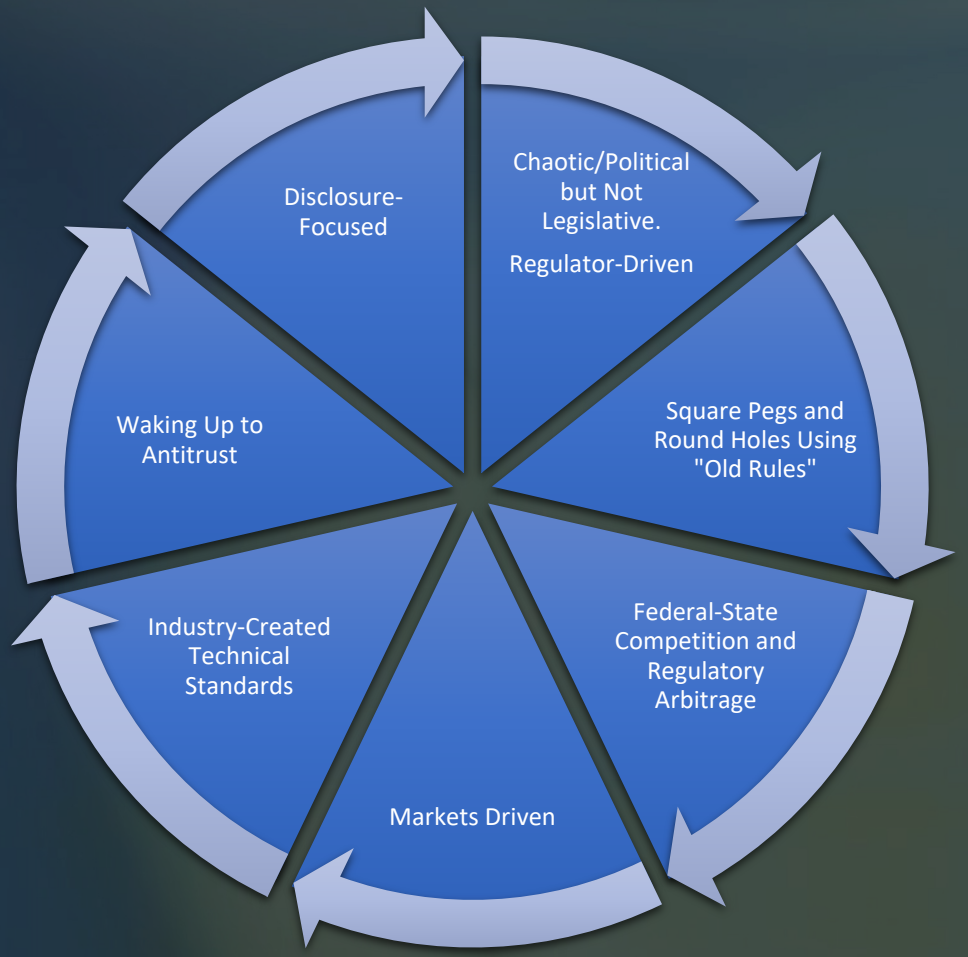
- **Fintech and Open Banking in the US and EU**
  - **Introduction**
  - **Understanding the Business Importance of Consumer Data to Fintech**
  - **Data Aggregation**
  - **Open Banking and Fintech**
  - **Top-Down Regulation: Mandated Open Banking in the EU**
  - **Privacy Law in the EU and the GDPR**
  - **Privately Negotiated or Government Mandated Open Banking in the US?**
  - **Financial Data Privacy Law in the US**

A Natural Experiment?

- Look for differences in regulatory approach between the US and the Eu
- What conclusions do you draw from those differences?

Questions?

US Approach to Fintech Regulation



Under US System, Fintechs

1

Negotiate to Access Critical Financial Rails

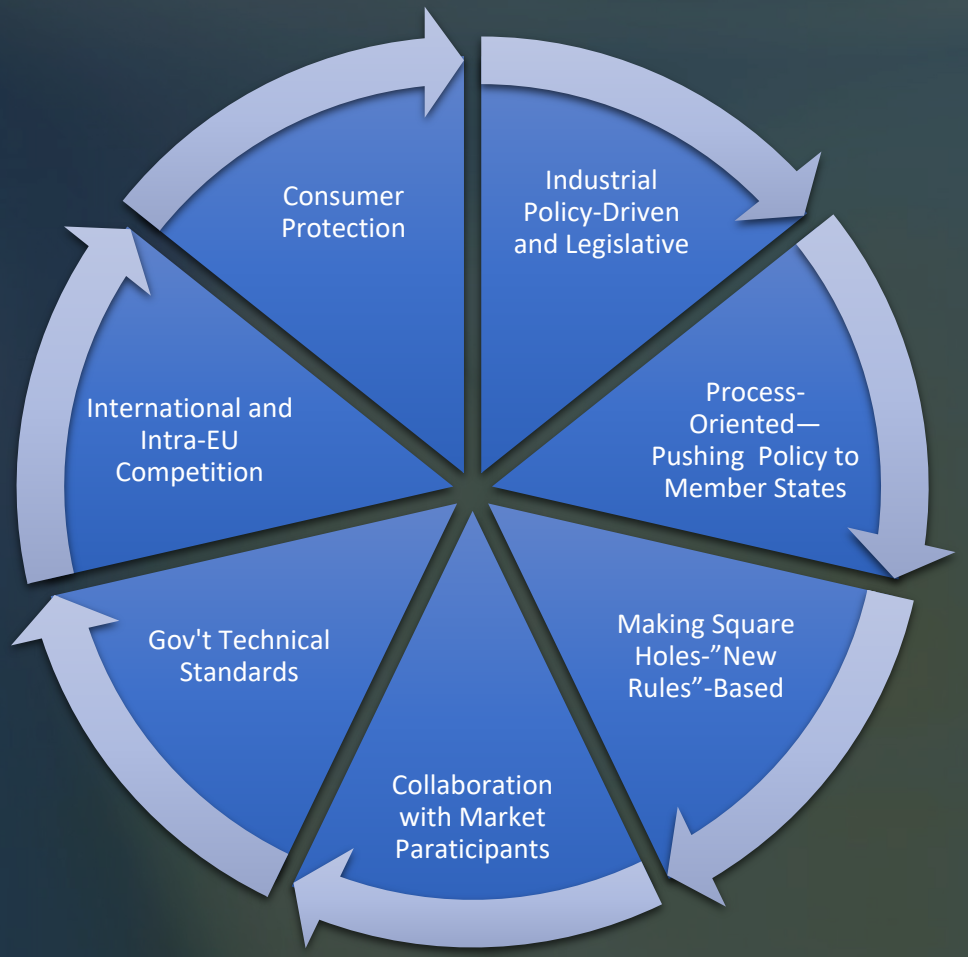
2

Compensate Oligopoly Toll Takers

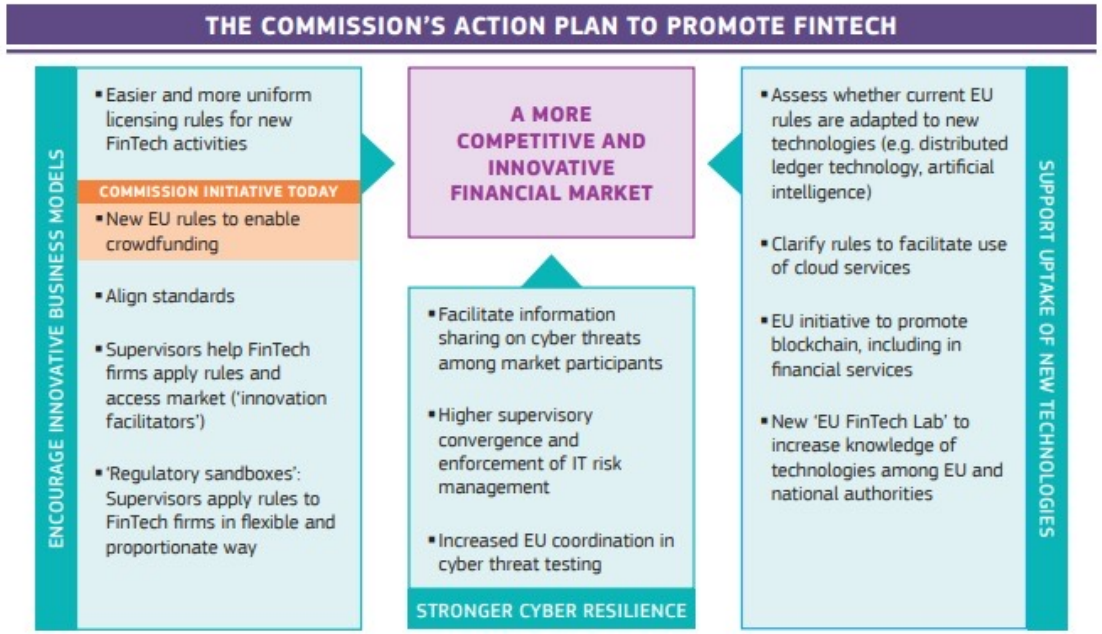
3

Seek Areas of Regulatory Arbitrage

EU Approach to Fintech Regulation



US Approach to Fintech Contrasts Sharply with EU Approach



BRIEFING

European Parliament

Fintech (financial technology) and the European Union

State of play and outlook

SUMMARY

The financial technology (fintech) sector encompasses firms that use technology-based systems either to provide financial services and products directly, or to make the financial system more efficient. Fintech is a rapidly growing sector: in the first half of 2018, investment in fintech companies in Europe alone reached US$26 billion.

The fintech sector brings rewards including innovation and job creation, but also challenges, such as data and consumer protection issues, and the risk of exacerbating financial volatility or cybercrime. To tackle these multi-disciplinary challenges, policy- and lawmakers in the European Union (EU) have adopted and announced several initiatives, for instance on intra-EU payment services, data protection, crowdfunding and regulatory sandboxes.

This briefing outlines current and upcoming fintech-related laws at EU level. It follows on from a March 2017 EPRS briefing that focused, inter alia, on the evolution, scope and economic prospects of fintech.

US Approach to Fintech Contrasts Sharply with EU Approach

Freshfields TQ

EU fintech regulation

Key themes in 2021

Setting global standards

The European Commission is taking its cue from GDPR – an export success story for European values and encouragement for global convergence.

This year, legislation on ethical and trustworthy AI, cryptoassets and operational resilience is expected to set the tone at international level.

Establishing 'strategic autonomy'

Facing disruptive international forces, strength in the digital ecosystem is a prerequisite for a geopolitical strategy.

The EU is looking to boost tech sovereignity whilst promoting growth and collaboration – for example via data sharing – leading to the new mantra of an 'open strategic autonomy'.

Guaranteeing a level playing field

Increasing international interdependencies and interconnectedness require high sensitivity in the creation of regulatory frameworks.

To continue enabling the protection of certain legal standards in addition to equal growth opportunities within the European Single Market, the application of regulation and enforcement is also required for third-country players.

Strengthening EU supervision

EU-level supervision is receiving strong tailwinds.

The planned introduction of a single EU AML supervisor, the regulation of the cryptoasset market including the supervision of stablecoins as well as the Lead Overseer concept in the Digital Operational Resilience Act are examples of this development.

Competition and digital policy collide

Co-ordinated competition enforcement efforts are promoting the EU's digital ambitions. This can be seen through an increasing linkage between competition and digital legislation.

Continuation of platform regulation and a framework for modernising digital markets and digital services are still to come.

Addressing entrance of BigTech in finance

Greater scrutiny of BigTech in finance is anticipated in 2021.

As an increasing suite of financial services is offered by technology companies, an inclusion in regulatory frameworks and supervisory mechanisms is foreseen.

The EU aims to co-ordinate fair antitrust investigations and emphasises application of the 'same activity, same risk, same rules' principle.

Freshfields Bruckhaus Deringer

Fintech

EU fintech regulation: key themes and trends

The digital transformation of financial services has created not only new ways of paying, lending and transferring money but also the potential to expose firms' technological frailties. In response, the EU is seeking ways to drive innovation in the financial sector while ensuring it can cope with cyber-related threats.

Europe's plans for digital finance

In September 2020, the European Commission launched its digital finance package, which includes:

- strategies for digital finance and retail payments; and
- proposed legislation for cryptoassets and digital operational resilience.

The package aims to:

- make Europe a global leader in – and standard-setter for – financial services;
- make more innovative financial products available to consumers; and
- ensure customer protection and financial stability.

Under EU System, Fintechs

1

Have Guaranteed Access Critical Financial Rails

2

Gov’t Defangs Toll Takers

3

Price: Submit to Regulation

Questions?

Let’s Dive a Little Deeper into One Issue for Contrast…

Understanding the Business Importance of Consumer Data to Fintech

--

It’s All About the Data

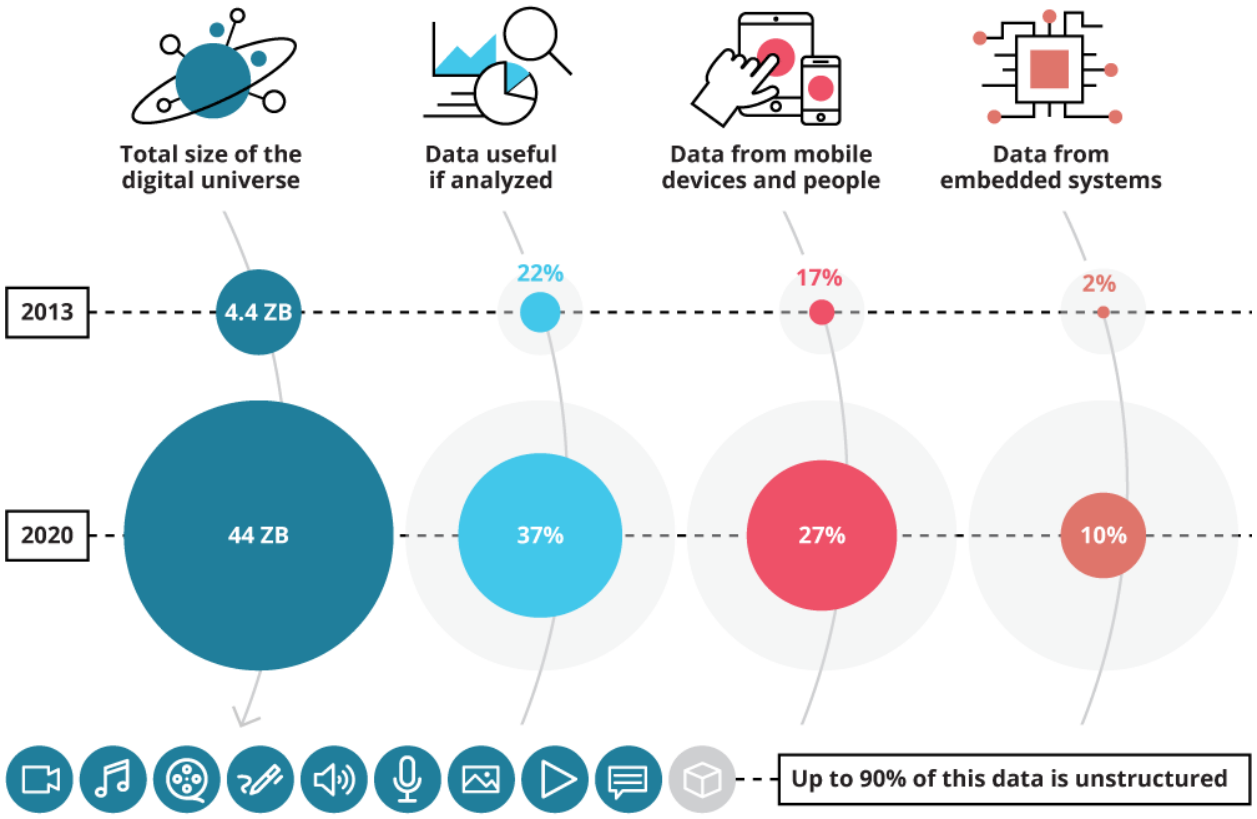
Consumer Financial Data is the <u>One Thing</u> Fintechs Absolutely Require to Succeed…

Why?

Fintech Creates Customer Value Through Technological Innovation

Figure 1. The expanding digital universe, 2013–2020

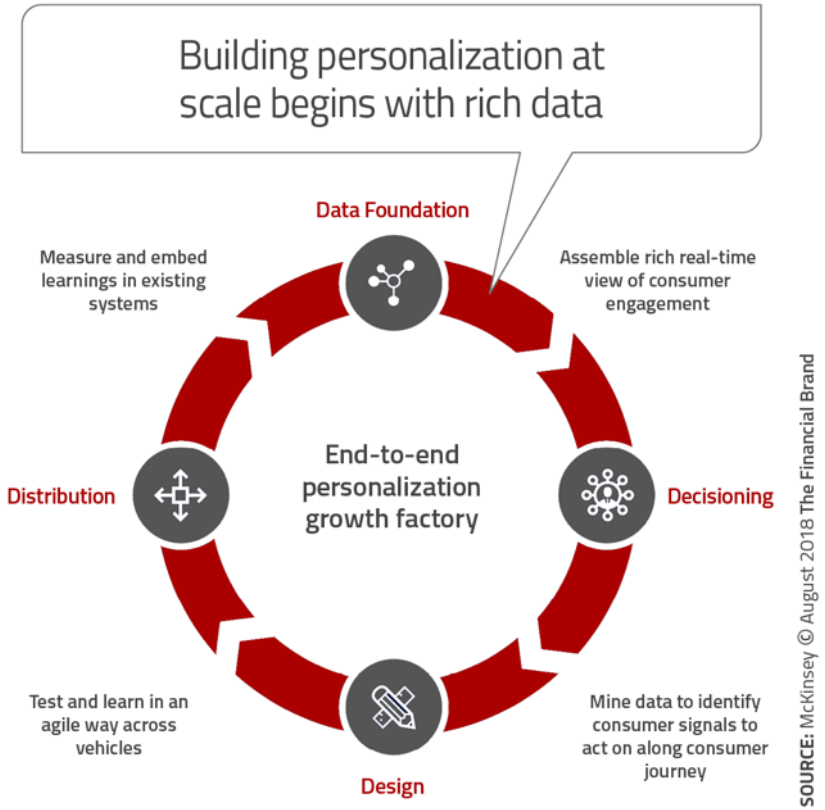
In 2020, the digital universe is expected to reach 44 zettabytes. One zettabyte is equal to one billion terabytes. Data valuable for enterprises, especially unstructured data from the Internet of Things and nontraditional sources, is projected to increase in absolute and relative sizes.

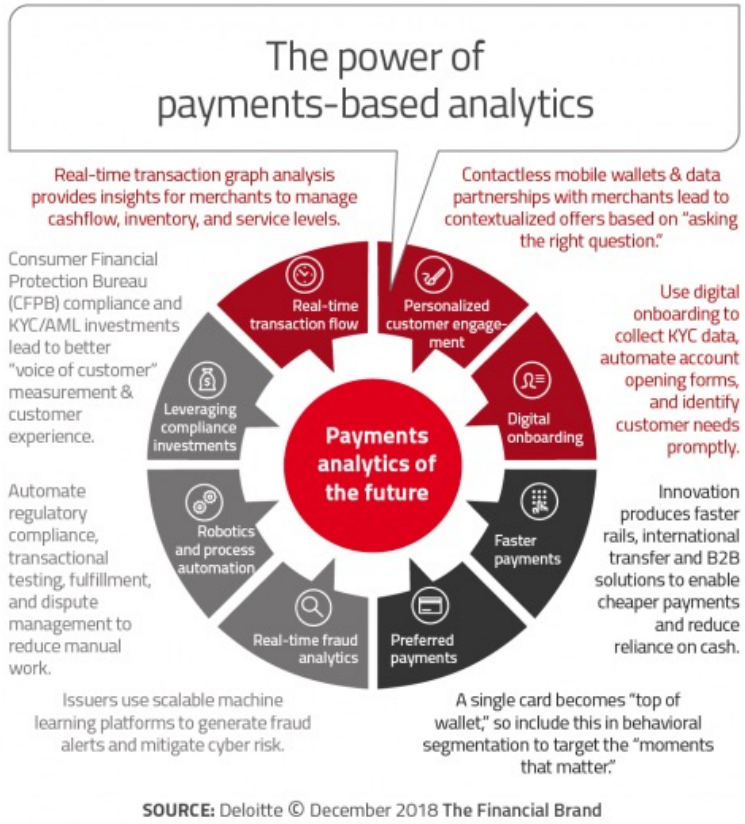


Sources: EMC Digital Universe with research and analysis by IDC, "The digital universe of opportunities: Rich data and the increasing value of the Internet of Things," April 2014; International Data Corporation, "IDC iView: Extracting value from chaos," 2011, www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf, accessed December 29, 2016.

The Data Revolution is the Driver

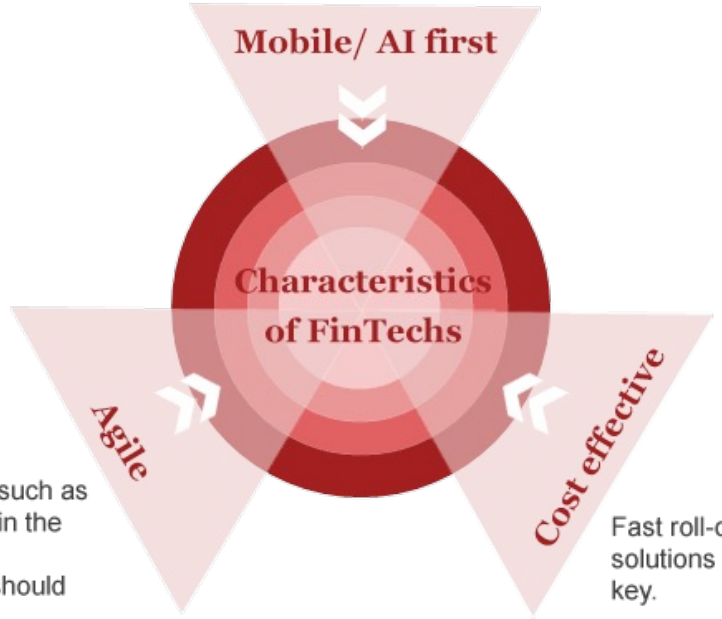
For Delivering Personalization and Analytics





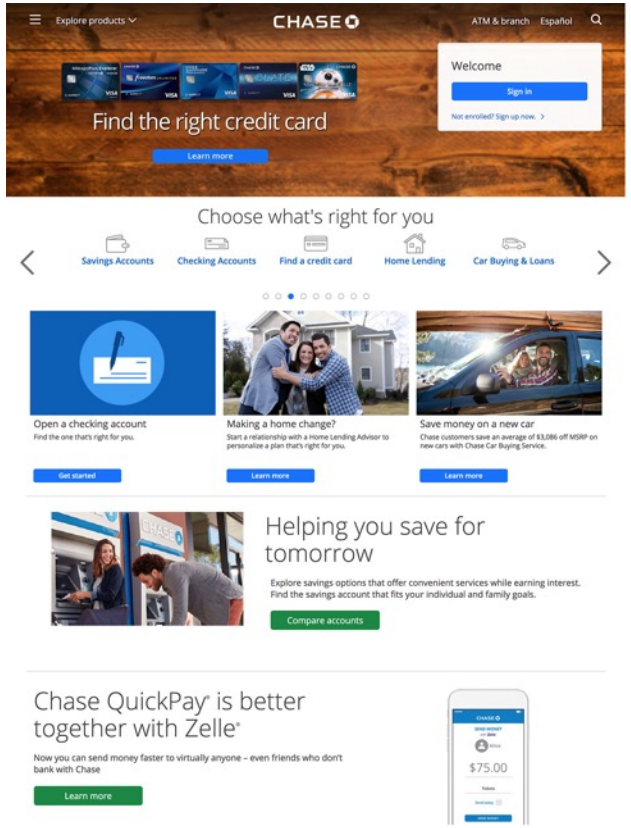
FinTech Relies on Superior Mobile & Online UI and UX

Offerings must be intelligent and able to adapt and address all user requirements at one go with no offline processing.

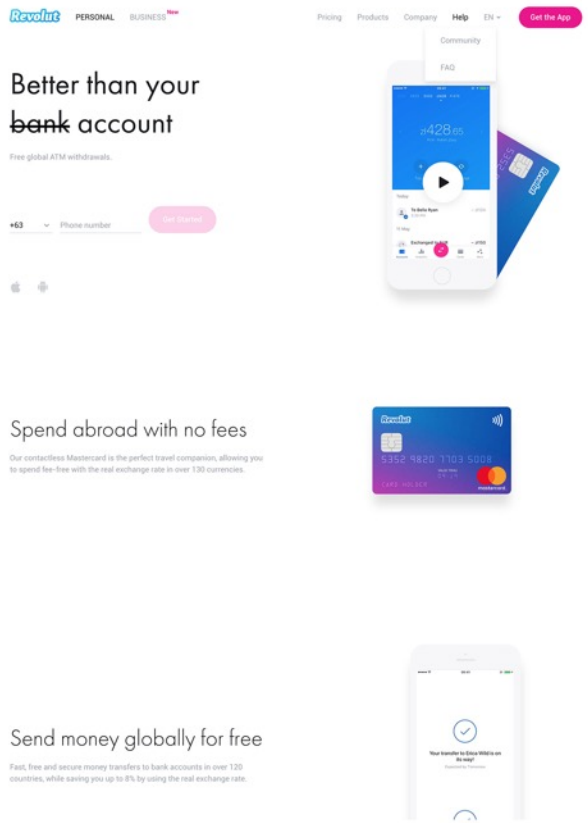


New age techniques such as Agile and Scrum are in the DNA of a FinTech.
The design process should factor in iterations.

Fast roll-out of market-ready solutions at optimum costs is key.

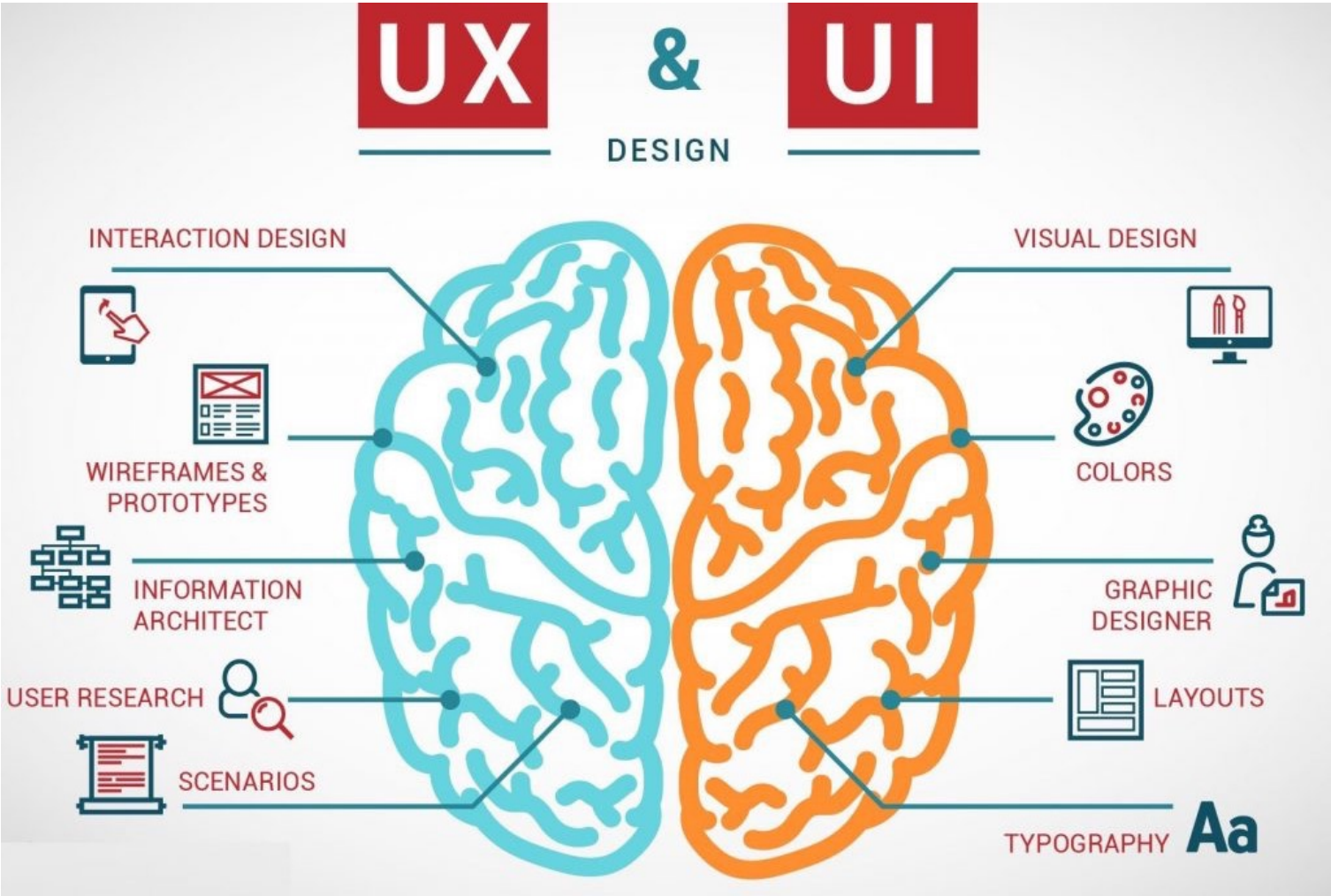


CHASE



REVOLUT

And Design Thinking…



And Artificial Intelligence and Machine Learning

All Fintech Products Require Personal Data to Work

DIGITAL MATURITY MODEL: PERSONAL FINANCE MANAGEMENT FEATURES

Less mature ← → More mature

Category	Showing	Analyzing	Enabling	Anticipating	Automating
Description	Aggregates and displays customers' financial data in one interface in new patterns without analyzing it.	Draws insights and generates advice from patterns found in users' financial data, provides suggestions on actions to take.	Enables customers to take action based on patterns in their financial data to modify and improve their financial health.	Blends forward-looking insights and action facilitation to help users make more long-term actions and better plan for the future. Makes suggestions before the need for them has arisen.	Uses predictive analytics and modeling to generate dynamic forward-looking insights to help users make informed decisions, then takes action based on those insights on their behalf (with permission).
Key Capabilities	• Account aggregation • Spending tracking • Spending auto-categorization • Financial data visualization (based only on past transactions) • Spending alerts & notifications	• Net worth analysis (based on current assets) • Suggestions on how to spend less on specific categories • Financial advice based on cash flow analysis	• Setting and adhering to saving goals • Setting and adhering to budgets • Merchant and transaction blocking • Subscription and recurring bill management • Applying for financial products and services digitally • Opening new financial accounts digitally	• Generating predictive financial insights based on current behavior patterns • Personalized offers based on transactions • Predictive credit decisions based on future as well as current income • Cash flow analysis (based on current and future income)	• Automatic adjustments to budgets, savings goals, and financial targets based on future life events • Automated savings (e.g. round-ups) • Automated portfolio adjustment (e.g. allocations) • Automated transfers between personal accounts

Source: Business Insider Intelligence conversations with PFM providers and software providers, December 2019-February 2020; The 2019 Retail Banking PFM Benchmark, Minna Technologies, 2019

BUSINESS INSIDER INTELLIGENCE

Most of this Data Comes from Banks or Other FIs

- Checking Account Transactional Data
- Savings Account Transactional Data
- Credit Card Transactional Data
- Loan and Other Credit Performance Data
- Rent and Subscription Payments Data
- Investment Activity Data

- Credit Bureau Data
- Marketing Database Data

Insights:

- Employment History
- Salary
- Net Worth
- Behavioral Characteristics
- Risk Tolerance
- Marital Status
- Credit Worthiness
- Etc.Etc.

What if Banks and FIs Don’t Want to Share Data?

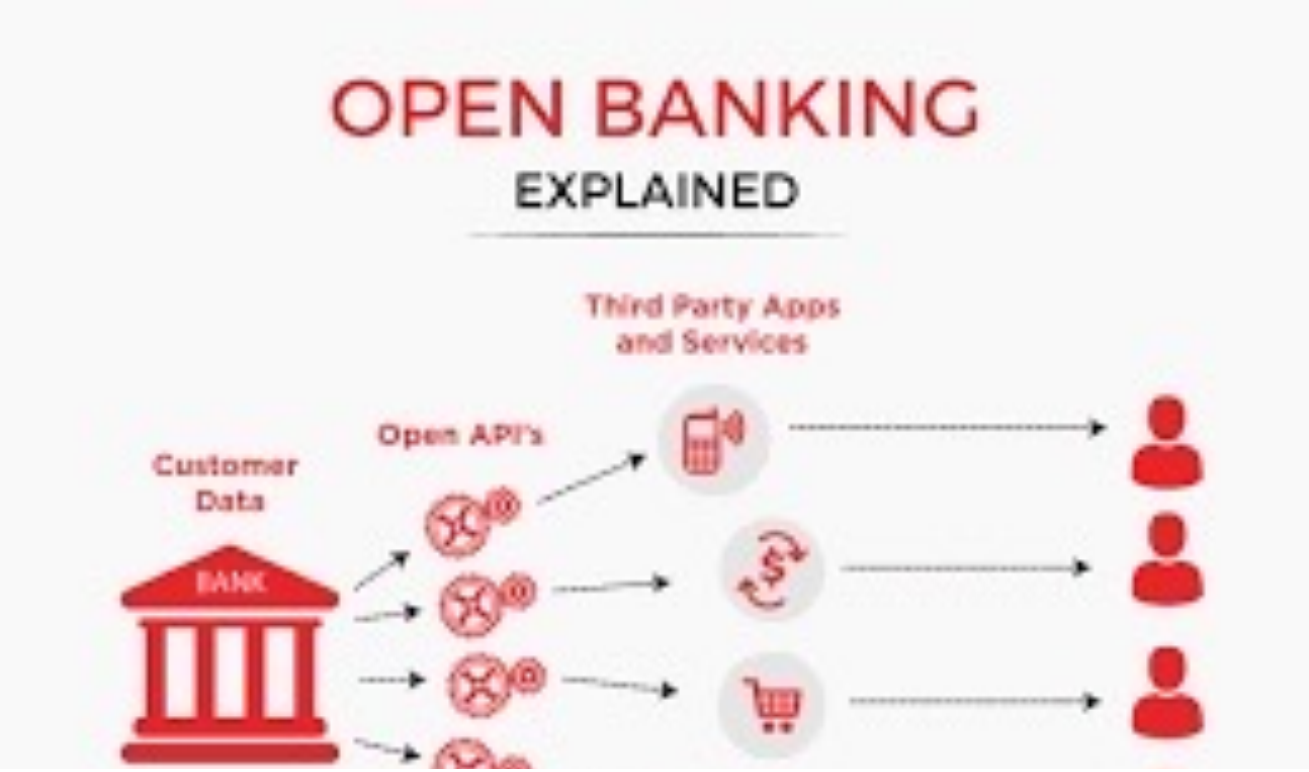
Questions?

Open Banking and Fintech

--

Fintech Relies on the Legal/Technological Concept of “Open Banking” to Access Data

- **Open banking** is a practice that provides third-party financial service providers like FinTech’s with access to **consumer banking, transaction, and other financial data** from banks and non-bank financial institutions, principally through use of **application programming interfaces (APIs)**.



“Open Banking” in Action at Digit

How does Digit save for me?

Digit looks at a few things when it determines when and how much to save for you:

- Linked bank account balance
- Upcoming income (paychecks or predicted irregular income)
- Upcoming bills
- Recent spending
- Any savings controls that you set (Overdraft Prevention, Safe Saving Level)

Every day that your bank is open, Digit uses this information to try and find amounts that you can spare. That money is then distributed into your different savings goals.

The funds in your Digit Account are held at FDIC-insured banks for your benefit and are protected up to a balance of $250,000.

Why do you need my bank login information?

Linking a bank to your Digit account

In order to save for you, Digit needs to be linked to an active bank account. Daily, Digit receives information from your bank on your balance and expenses to determine when and how much to save.

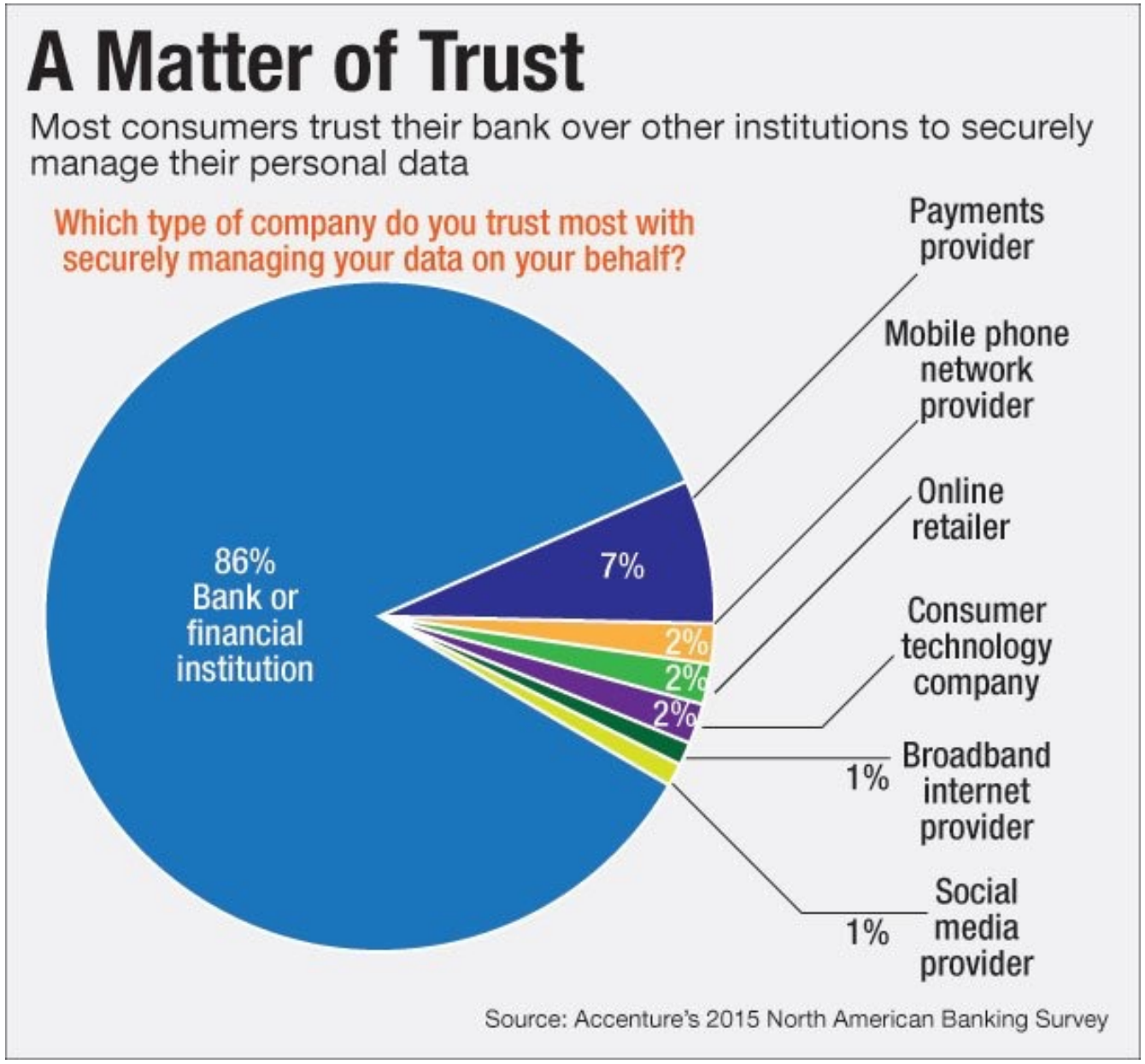
Digit links with your bank account by using the same info that you would use to sign in to your online banking either on your bank's website or through their mobile app.

We use a trusted and industry-standard data provider to handle connections between Digit and your bank. Additionally, we practice several levels of security to ensure that your data and money are always safe.

Banks Generally Fear Open Banking

- **The banking value chain is changing**.
- Fintech startups are building digitally streamlined services with banks' data and attracting customers away from the banks, effectively breaking up the traditional banking value chain.
- **The role of the bank as intermediary between customer and retailer in processing payment processes becomes superfluous.**
- Instead, the customer confirms the transaction directly with the purchase using two-factor authentication, the money flows from his account to that of the merchant.
- **For financial institutions, therefore, there is an acute risk of loss of relevance, since they may only serve as an interchangeable backend for the technical and logistical processing of payments.**

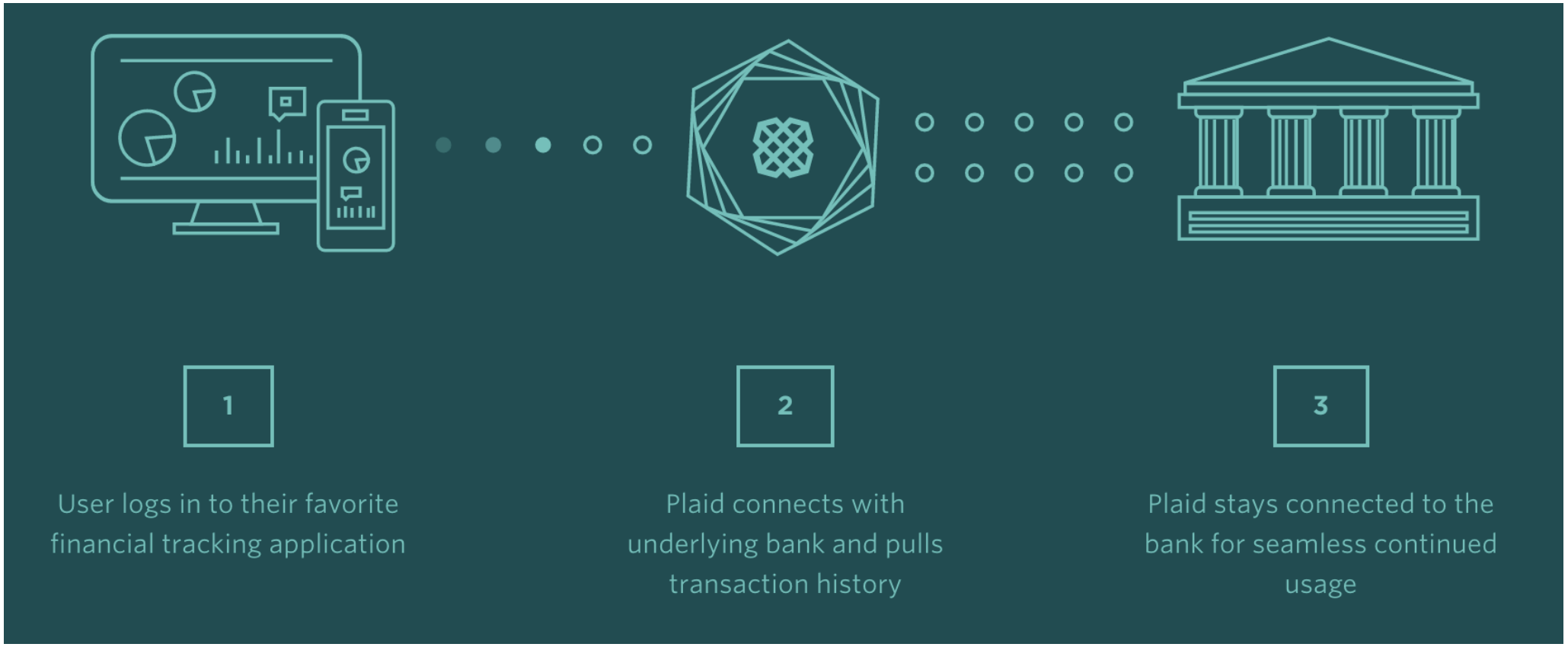
But Banks Retain a Trust Advantage



Aggregators

- Aggregators pull data from financial institutions via screen scraping or APIs (Application Programming Interface, a software intermediary that allows two applications to talk to each other), clean and organize/structure the data, and retransmit it via API to customers such as fintech apps, other financial institutions, and hedge funds.
- Aggregators receive **permissio**n to collect consumer data through their partnerships with fintech apps or other end user platforms. These apps' terms of use and customer contracts require customer permission to access their accounts.
    - However, once the aggregators obtain the customer data, it may be de-identified and used for other purposes.
- The largest account aggregators include **Plaid, Finicity, Yodlee and MX**.

Role of Aggregators

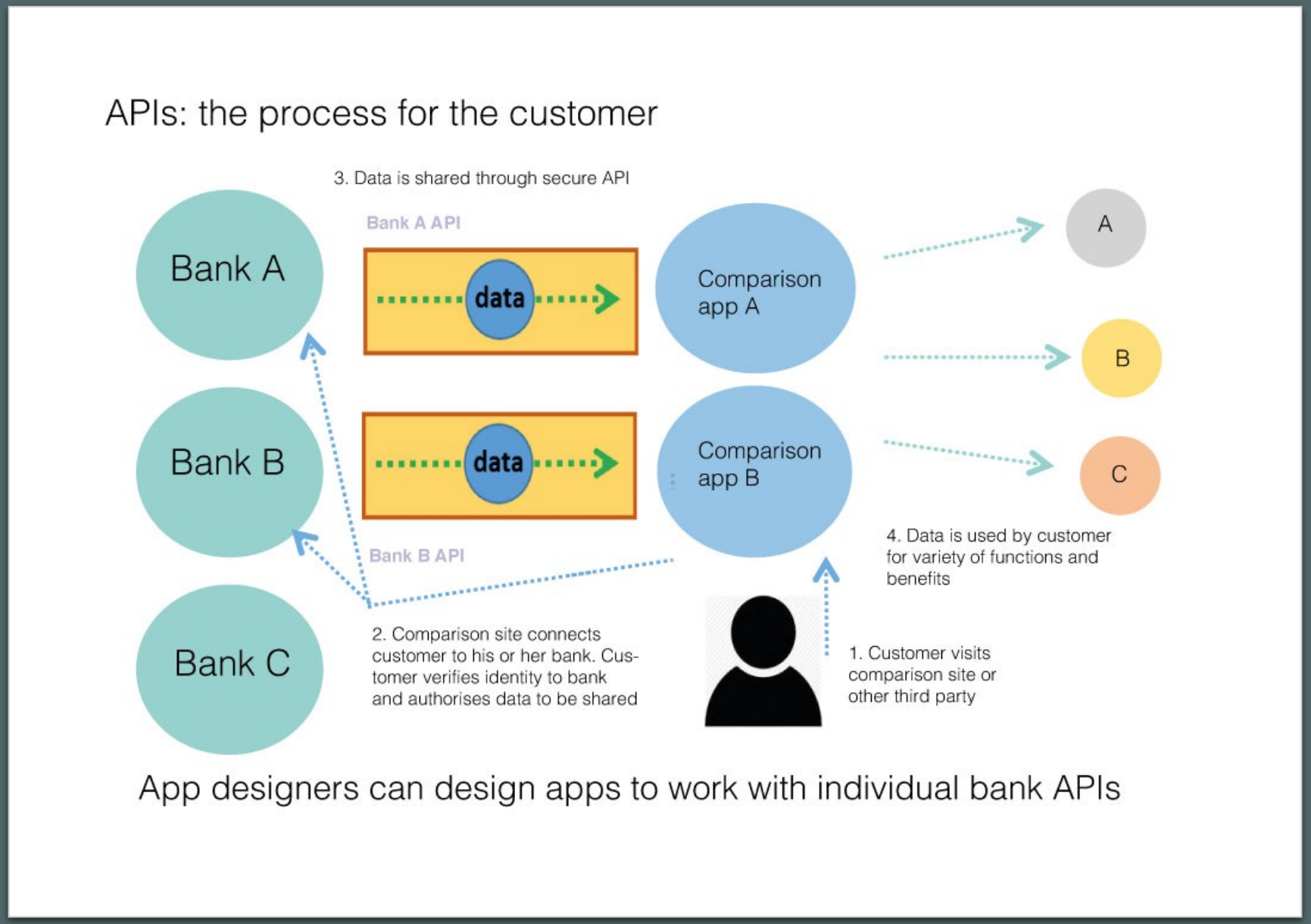


Screen Scraping is How Aggregators Started

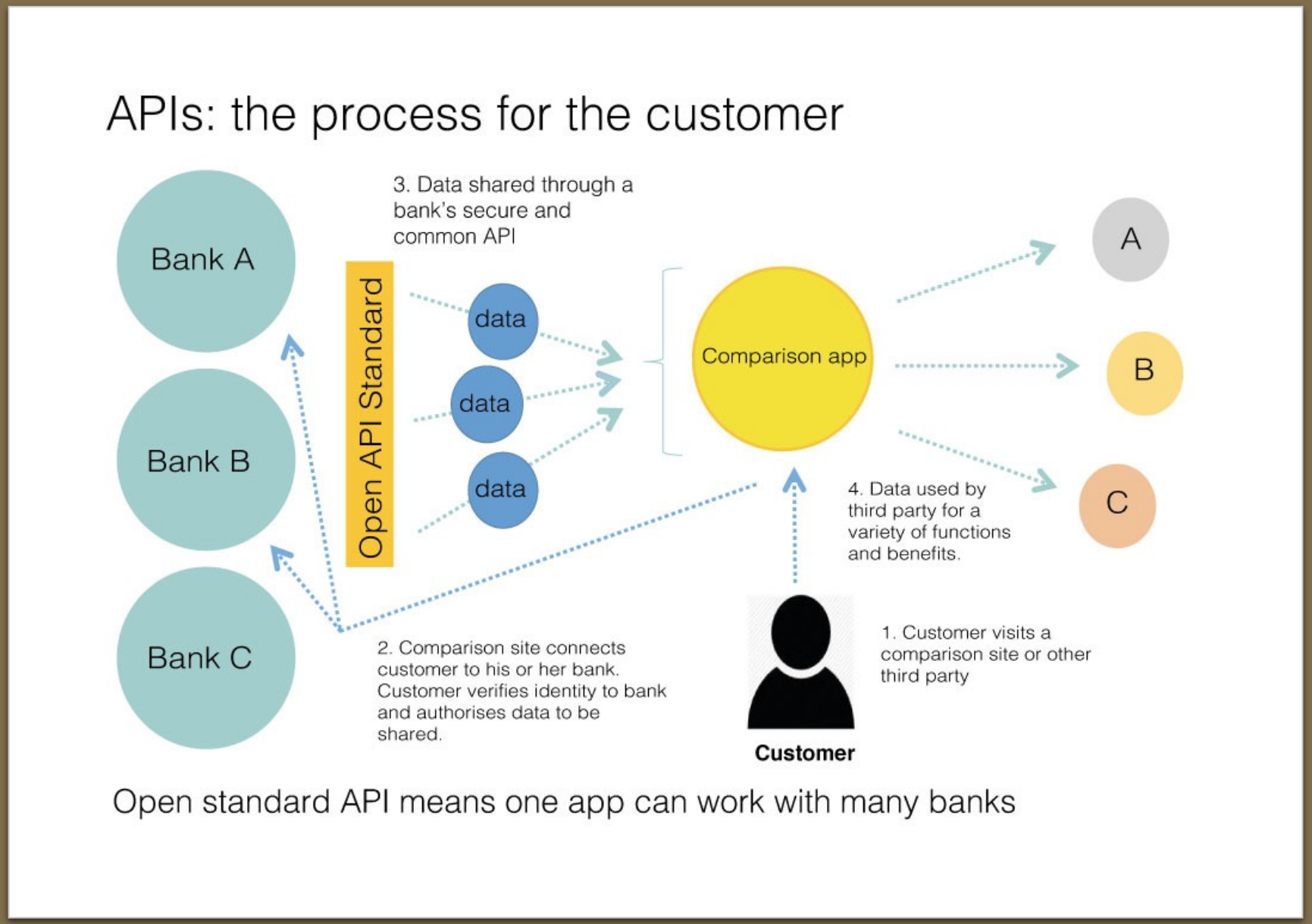
- Screen-scraping allows third party aggregators to access bank and brokerage accounts on a client's behalf **using the client's access credentials (login/pw)**.

The Better Alternative is an API

- API is the acronym for **Application Programming Interface**, which is a software intermediary that allows two applications to talk to each other.
- Each time you use a mobile app like Facebook, send an instant message, or check the weather on your phone, you're using an API.
- An API is a software-to-software interface, not a user interface. With APIs, applications talk to each other without any user knowledge or intervention.
- When you buy movie tickets online and enter your credit card information, the movie ticket website uses an API to send your credit card information to a remote application that verifies whether your information is correct. Once payment is confirmed, the remote application sends a response back to the movie ticket Web site saying it's OK to issue the tickets.
- **With an API, your phone's data is never fully exposed to the server, and likewise the server is never fully exposed to your phone. Instead, each communicates with small packets of data, sharing only that which is necessary**.



Two Types of API: Dedicated Bank API



Two Types of API: Open API

Questions?

Aggretators

--

Plaid: Leading US Data Aggregator

What is Plaid?

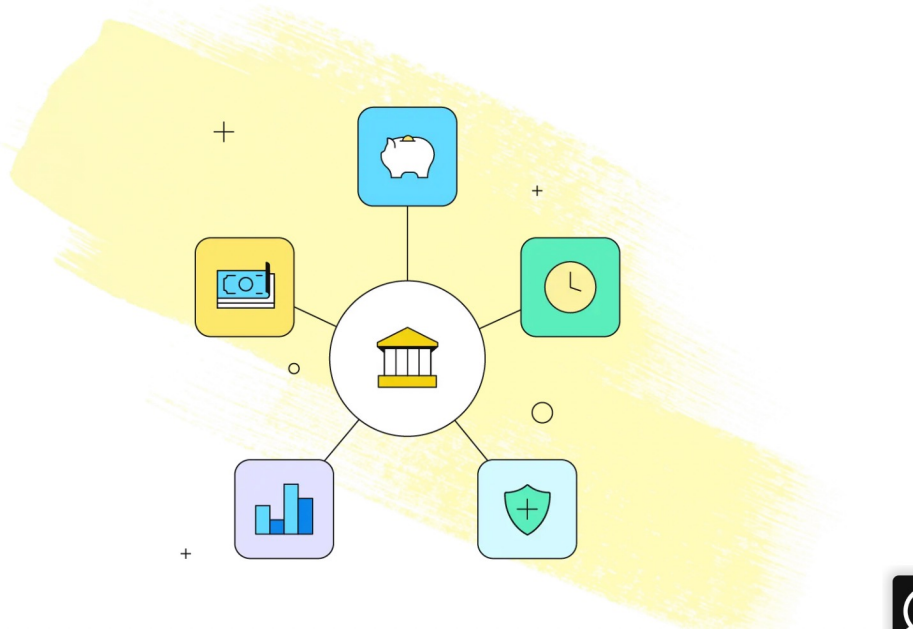
Plaid makes it easy to securely connect your bank to the apps you want to use

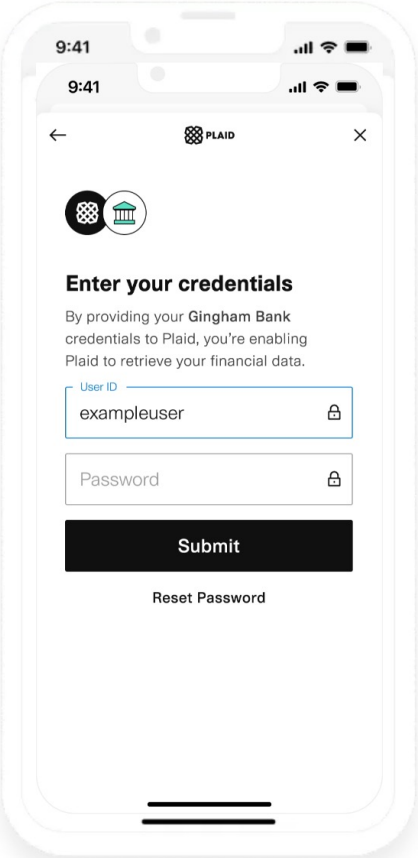
Connecting your bank to your apps

We power thousands of the apps that people rely on to manage their financial lives.

- **Venmo** (peer-to-peer payments)
- **Betterment** (automated investing)
- **Chime** (online banking)
- **Dave** (earned wage access)
- And thousands more...

Meet companies powered by Plaid ›





How it works

We connect to 11,000 financial institutions across the United States, Canada, and Europe. With Plaid, connecting your bank account is easy:

- **Step 1**
  When you sign up with a Plaid-powered app, you'll be able to select your financial institution from a list. Then, enter your login and password.
- **Step 2**
  In a matter of seconds, we encrypt the data you've chosen to share (for instance, your account balance) and securely share it with the app you want to use. We never share your login and password with the app.
- **Step 3**
  We work behind the scenes to build a secure, ongoing connection between the app and your bank.

Learn more about our company ›

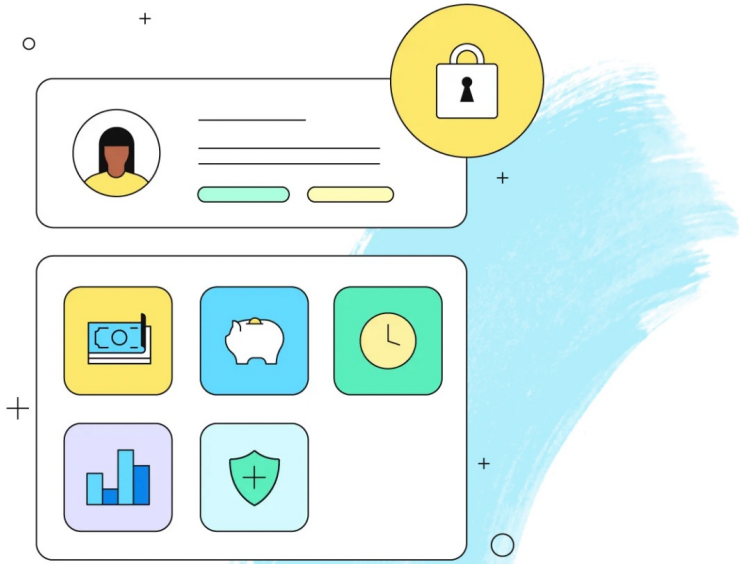
Plaid: Leading US Data Aggregator

Your data, your choice

With Plaid, you're in control. You choose whom your data is shared with, for what purpose, and how long. Some of the most common information we help people share includes:

- Account and routing number
- Account balance
- Transaction history
- Personal loans and credit cards
- Investment holdings
- Identity information (to prevent fraud)

Learn about our data practices and policies ›

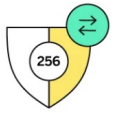


Plaid: Leading US Data Aggregator

Protecting your data

Whenever you use a Plaid-powered app, we're working behind the scenes to protect your financial information. Our security practices are designed to meet or exceed the industry standards that banks and leading technology companies use. They include:

Learn about our security policy ›

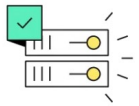


End-to-end data encryption

The combination of the Advanced Encryption Standard (AES-256) and Transport Layer Security (TLS) help keep your personal information safe end-to-end.

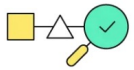
Strong authentication

Plaid protects your data on our systems and requires multi-factor authentication for added security.



Cloud infrastructure

Plaid uses secure cloud infrastructure technologies to enable you to connect quickly and safely.



Robust monitoring

The Plaid API and all related components are continuously monitored by our information security team.

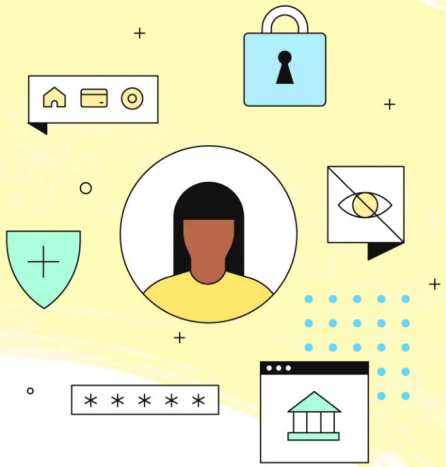
Plaid: Leading US Data Aggregator

You're in control

Your data belongs to you. That means:

- **We don't sell your data** to any outside companies.
- **We don't share your data** with anyone without your permission.
- **You're in control** of whom you share your data with and for how long.

Learn about our data practices and policies ›



Plaid: Leading US Data Aggregator

Products

Learn how you can make the most of financial data

Global coverage ›

Auth ›

Account and routing numbers

Assets ›

Point-in-time snapshots of users' finances

Identity Verification ›

Global KYC and anti-fraud

Balance ›

Real-time balance checks

Income ›

Income and employment verification

Monitor ›

AML and PEP screening

Identity ›

Bank account-holder information

Investments ›

Retirement, brokerage, and crypto data

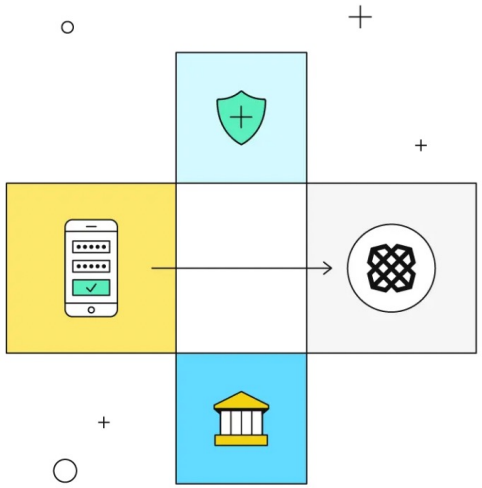
Transactions ›

Up to 24 months of categorized data

Liabilities ›

Student loan, credit card, and mortgage data

Plaid: Leading US Data Aggregator



How Plaid makes money

When you connect your financial data to an app or service, they pay Plaid. For example, when you add a bank account to Square Cash, they pay us a fee.

Plaid is free for everyone who uses a Plaid-powered app, allowing you to securely connect your bank account to the apps you want in just a few seconds.

Meet companies powered by Plaid ›

Plaid: Leading US Data Aggregator

Where Plaid is used: Examples

Plaid has a variety of different use cases. It can be used to evaluate your credit, verify income or confirm sufficient funds for peer-to-peer payments, to name a few.

Some examples of institutions that use Plaid include:

- **NerdWallet:** NerdWallet's app allows you to track net worth, cash flow, credit score and more, but in order to get that information you have to link financial accounts through Plaid.
- **Venmo:** The mobile app for peer-to-peer payments and money transfers requires you to verify a bank account through Plaid by entering a username and password for an online bank account. Venmo uses that to verify the account information and balance to see whether there is enough money to cover a transaction.
- **Chime:** By providing Plaid with login credentials to an eligible external bank account, it may be possible to use it to fund your Chime bank account.
- **Petal and TomoCredit:** When applying for the Petal credit card or Tomo Card, you may be required to link a bank account through Plaid during the application process to provide a more holistic view of your finances.

Plaid: Leading US Data Aggregator

Build your financial life

Your financial data is powerful. It can help you pay down debts, save for retirement, and make progress toward your goals. With Plaid-powered apps, you can:

Invest your spare change in the stock market

Meet Acorns ›

Subscribe to a service that will keep you from overdrafting

Meet Dave ›

Consolidate your credit card debt so you never miss a payment

Meet Tally ›

Plaid: Leading US Data Aggregator

Visa to buy Swedish fintech Tink for $2.1 billion after abandoning Plaid takeover

PUBLISHED THU, JUN 24 2021•3:13 AM EDT | UPDATED MON, JUN 28 2021•10:17 AM EDT

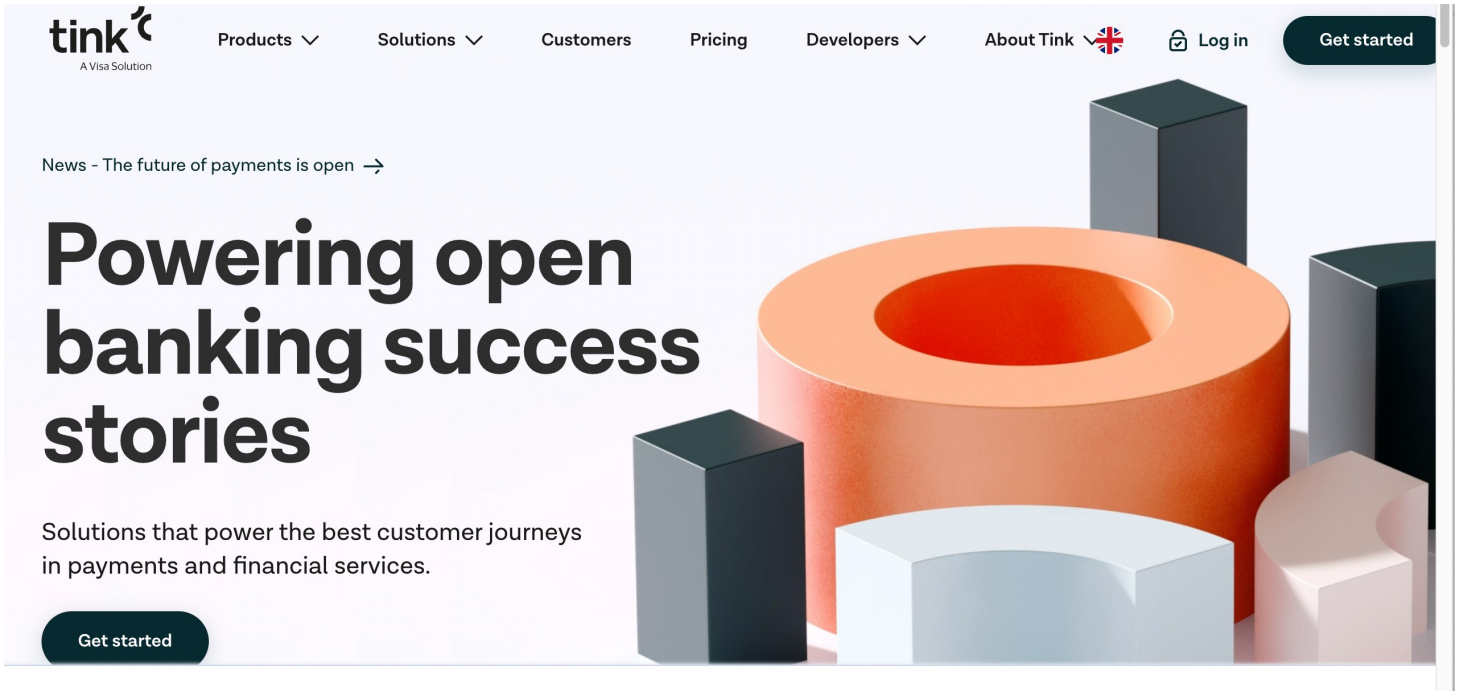
Ryan Browne
@RYAN_BROWNE_

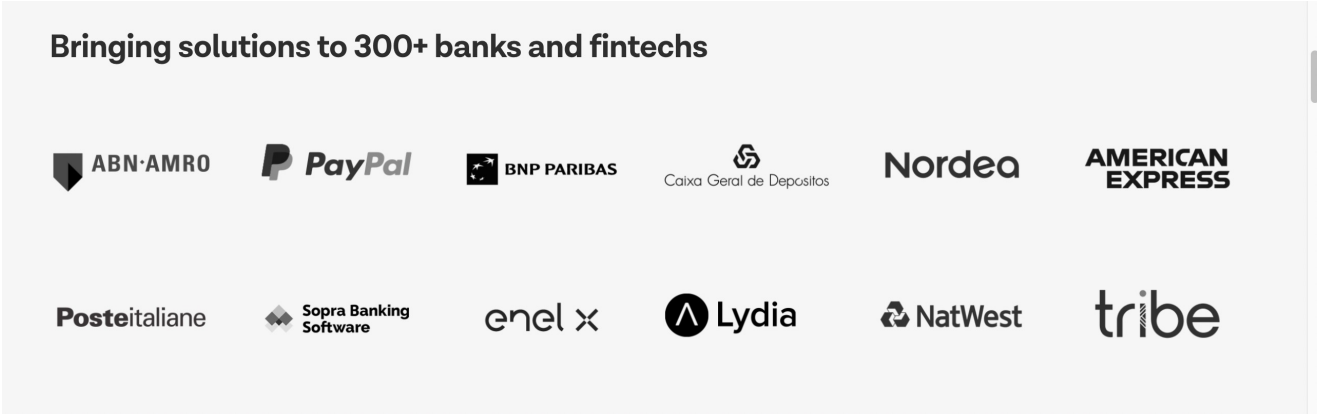
SHARE

KEY POINTS

- Visa has agreed to acquire Swedish financial technology start-up Tink for 1.8 billion euros ($2.1 billion).
- The deal comes after Visa's bid to buy Plaid, an American rival to Tink, was torpedoed by U.S. regulators.
- Plaid and Tink both operate in a nascent space known as open banking.

Plaid, Visa and Tink


tink
A Visa Solution
Products
Solutions
Customers
Pricing
Developers
About Tink
Log in
Get started
News - The future of payments is open
Powering open banking success stories
Solutions that power the best customer journeys in payments and financial services.
Get started


Bringing solutions to 300+ banks and fintechs
ABN·AMRO
PayPal
BNP PARIBAS
Caixa Geral de Depositos
Nordea
AMERICAN EXPRESS
Posteitaliane
Sopra Banking Software
enel x
Lydia
NatWest
tribe

Tink

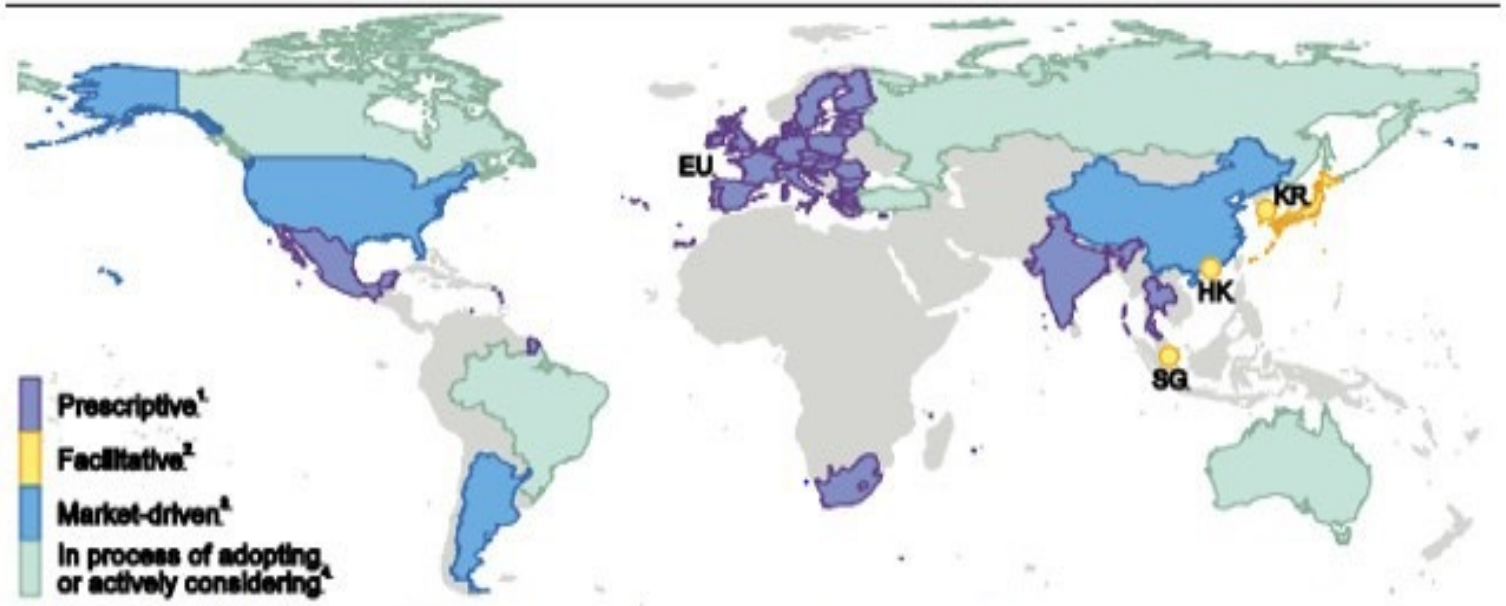
Klarna launches new Klarna Kosma division for its open banking platform

Romain Dillet @romaindillet / 3:00 AM EDT • March 31, 2022

Comment

Klarna

Questions?



The boundaries shown and the designations used on this map do not imply official endorsement or acceptance by the BIS.

EU = European Union, HK = Hong Kong SAR, KR = Korea, SG = Singapore.

[1] Requires data sharing, [2] Encourages data sharing, [3] No explicit rule/guidance requiring data sharing, [4] In process of adopting or actively considering adopting.

Source: Based on information gathered from Committee jurisdictions

Source: FiServ.

Open Banking Around the World

Top-Down Regulation: Mandated Open Banking in the EU

--

What is PSD2?

The revised Payment Services Directive (PSD2) went into effect 2018 across the EU (including UK).

PSD2 requires banks to provide free interfaces for exchanging data with regulated external providers.

PSD2 allows certain third-party providers (TPPs) to directly access payment service users' online payment accounts with their explicit consent, and requires Account Servicing Payment Service Providers (ASPSPs), such as banks, to permit access through a dedicated interface built on APIs.

APIs allow TPPs to access information about accounts, transactions and payments without any individual contractual agreements with the bank

PSD2 was designed to open up the banking industry to new players and promote the development and use of innovative online services, while ensuring consumer protection.

PSD2 provides the legislative and regulatory foundation for Open Banking and other broader initiatives at a UK and European level relating to open access to payment accounts.

Top-Down Technical Standards

OPEN BANKING

API Specifications | Security Profiles | Customer Experience Guidelines | Operational Guidelines | Other Guidelines | Reference Library

Guidance when implementing the Standard

Where any part of the Open Banking Standard (API Specifications, Security Profiles, Customer Experience Guidelines and Checklist and Operational Guidelines and Checklist) is being implement
either an ASPSP or a TPP, the following categorisation is applied:

Mandatory (required in all cases)

Functionality, customer experience and operational guidelines marked as 'Mandatory', 'Required' or 'Must' will be implemented in all cases for regulatory compliance and/or for the API to function and deliver essential customer outcomes.

Where relevant, these requirements are marked as Mandatory for PSD2 (for all ASPSPs) and/or the CMA Order (for CMA9 PCA/BCA accounts).

For functionalities and endpoints:
*• An ASPSP **must** implement an endpoint that is marked Mandatory.*
*• An ASPSP **must** implement functionality that is marked Mandatory.*
For fields:
*• A TPP **must** specify the value of a Mandatory field.*
*• An ASPSP **must** process a Mandatory field when provided by the TPP in an API request.*
*• An ASPSP **must** include meaningful values for Mandatory fields in an API response.*

Conditional (required in some cases)

Functionality, customer experience and operational guidelines marked as 'Conditional' may also need to be implemented in some cases for regulatory compliance (for example, if these are made available to the PSU in the ASPSP's existing Online Channel).

For functionalities and endpoints:
*• An ASPSP **must** implement functionality and endpoints marked as Conditional if these are required for regulatory compliance.*
For fields:
• All fields that are not marked as Mandatory are Conditional.
*• A TPP **may** specify the value of a Conditional field.*
*• An ASPSP **must** process a Conditional field when provided by the TPP in an API request, and must respond with an error if it cannot support a particular value of a Conditional field.*
*• An ASPSP **must** include meaningful values for Conditional fields in an API response if these are required for regulatory compliance.*

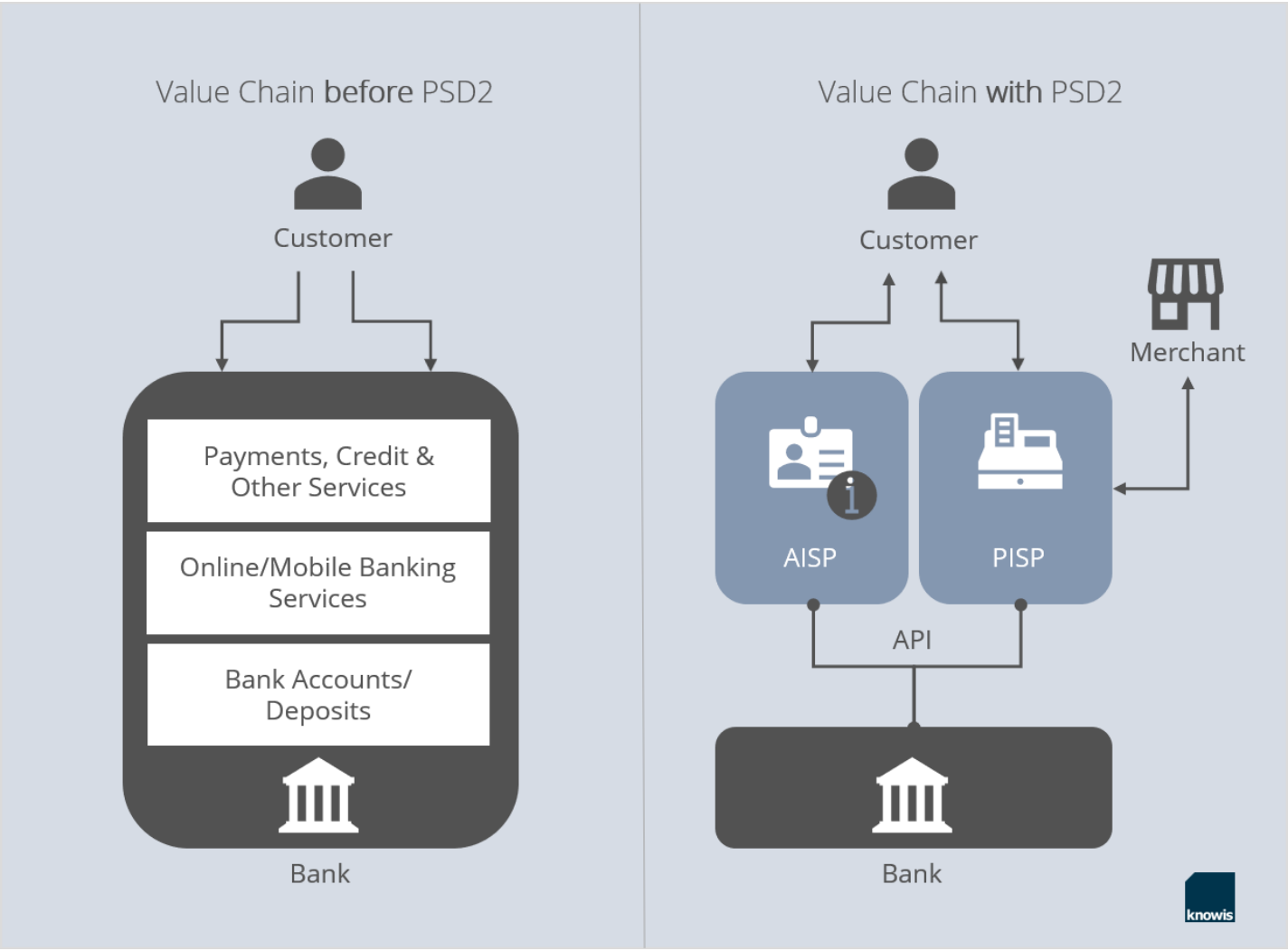
Optional

Functionality, customer experience and operational guidelines marked as 'Recommended' or 'Should' are n
necessarily required for regulatory compliance but should be implemented where possible to enable desir
customer outcomes. Those marked as 'Optional' or 'Could' may deliver further desired outcomes.
For functionalities and endpoints:
*• An ASPSP **may** implement an Optional endpoint.*
*• An ASPSP **may** implement Optional functionality.*
For fields:
• There are no Optional fields.
• For any endpoints which are implemented by an ASPSP,
fields are either Mandatory or Conditional.

Notes

• If an ASPSP has deviated from implementing functionality classified as mandatory or conditional (where applicable) and is seeking an exemption, they will need to explain this divergence to thei
NCA

Open Banking Value Chain



Core Concepts of PSD2

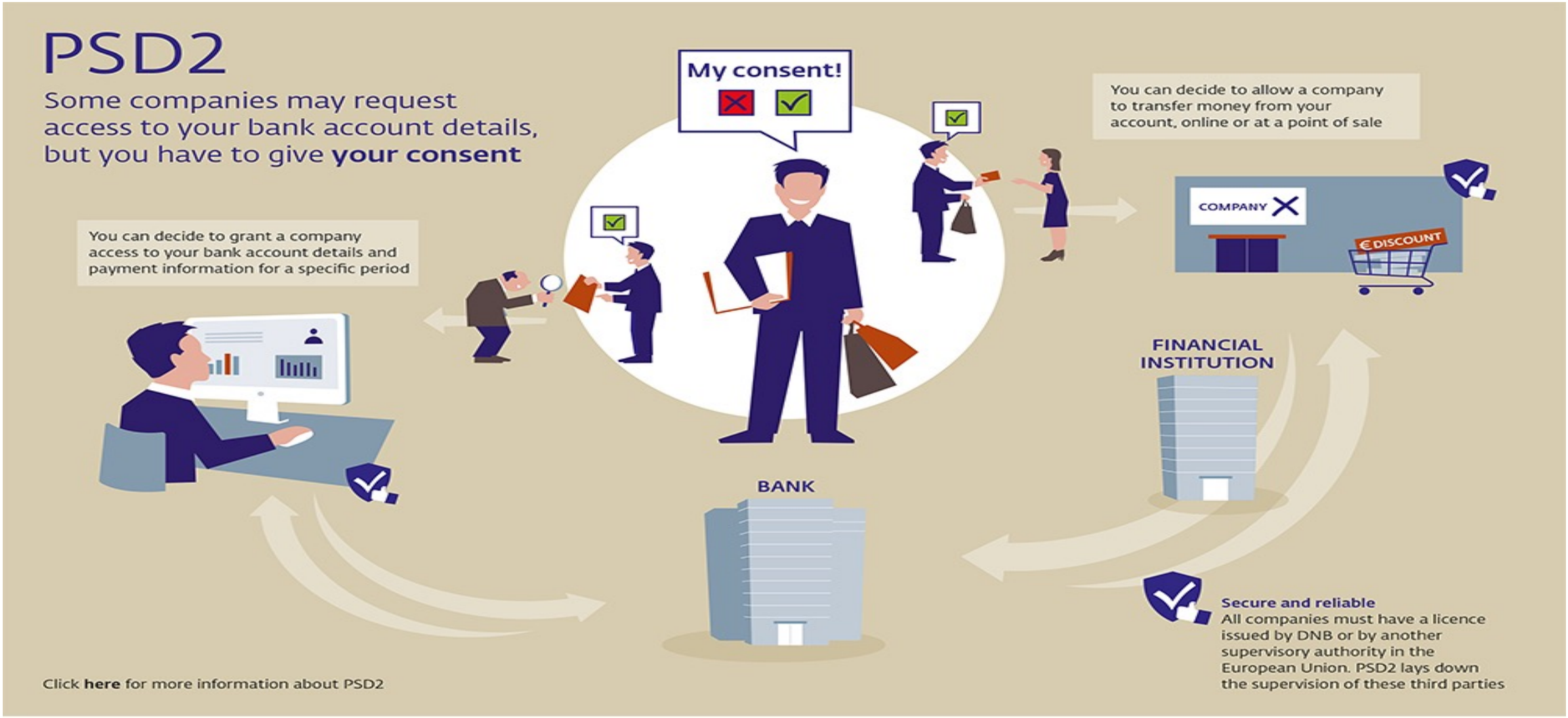
AIS

- What is AIS?
- Under PSD2, an Account Information Service (AIS) is an online service that provides consolidated information to a user on one or more payment accounts held by that user with other payment service providers. Firms that are registered or authorised to provide account information services can, with the explicit consent of the end consumer, access their bank account to provide the end consumer with new products and services.

PIS

- What is PIS?
- Under PSD2, a Payment Initiation Service (PIS) is an online service which accesses a user's payment account to initiate the transfer of funds on their behalf with the user's explicit consent and authentication.

Open Banking Customer Perspective



DeNederlandscheBank EUROSYSTEEM | NFPS National Forum on the Payment System

PSD2, the new European payment services directive

The EU View: PSD2 Brings Major Consumer Benefits

- PSD2 tackles fraud in online payments: PSD2 introduces strong security requirements for electronic payments and for the protection of consumers' financial data to ensure their privacy is respected by all market operators. These rules should boost consumer confidence when buying online;
- PSD2 opens the EU payment market to competition: PSD2 sets the stage for the future. With online financial services constantly evolving, the new rules will apply equally to traditional banks and to innovative payment services and new providers, such as FinTechs. These players, also called third party payment service providers (TPPs), will now be regulated under EU rules. They will be able to bring a wealth of consumer benefits. For instance, they can initiate payments on behalf of customers. They give assurance to retailers that the money is on its way, or give an overview of available accounts and balances to their customers;
- PSD2 increases consumers' rights in numerous areas. These include reducing consumers' liability for unauthorised payments and introducing an unconditional ("no questions asked") refund right for direct debits in euro;
- PSD2 prohibits surcharging, which is additional charges for payments with consumer credit or debit cards, both in shops or online;
- PSD2 improves complaints procedure - PSD2 obliges Member States to designate competent authorities to handle complaints from payment service users and other interested parties, such as consumer associations, if they consider their rights established by the Directive have not been respected.

The Big Techs are Using PSD2 in Europe

Firm	Year payment-related licence acquired	EEA National Competent Authority
PayPal (Europe) S. à.r.l	2007 (Banking Licence)	CSSF (Luxembourg)
Amazon Payment Europe S.C.A	2010	CSSF (Luxembourg)
eBay S. à.r.l	2014	CSSF (Luxembourg)
Rakuten Europe Bank	2016 (Banking Licence)	CSSF (Luxembourg)
Implementation of PSD2		
Facebook Payments Intl Ltd	2018	Central Bank of Ireland (Ireland)
Alipay (Europe) Limited S.A.	2018	CSSF (Luxembourg)
Airbnb Payments UK Ltd	2018	FCA (United Kingdom)[14]
Google Payment Lithuania UAB	2018	Lietuvos Bankas (Lithuania)
Uber Payments B.V.	2019	De Nederlandsche Bank (Netherlands)

Source: EBA register of payment and electronic money institutions under PSD2.

Questions?

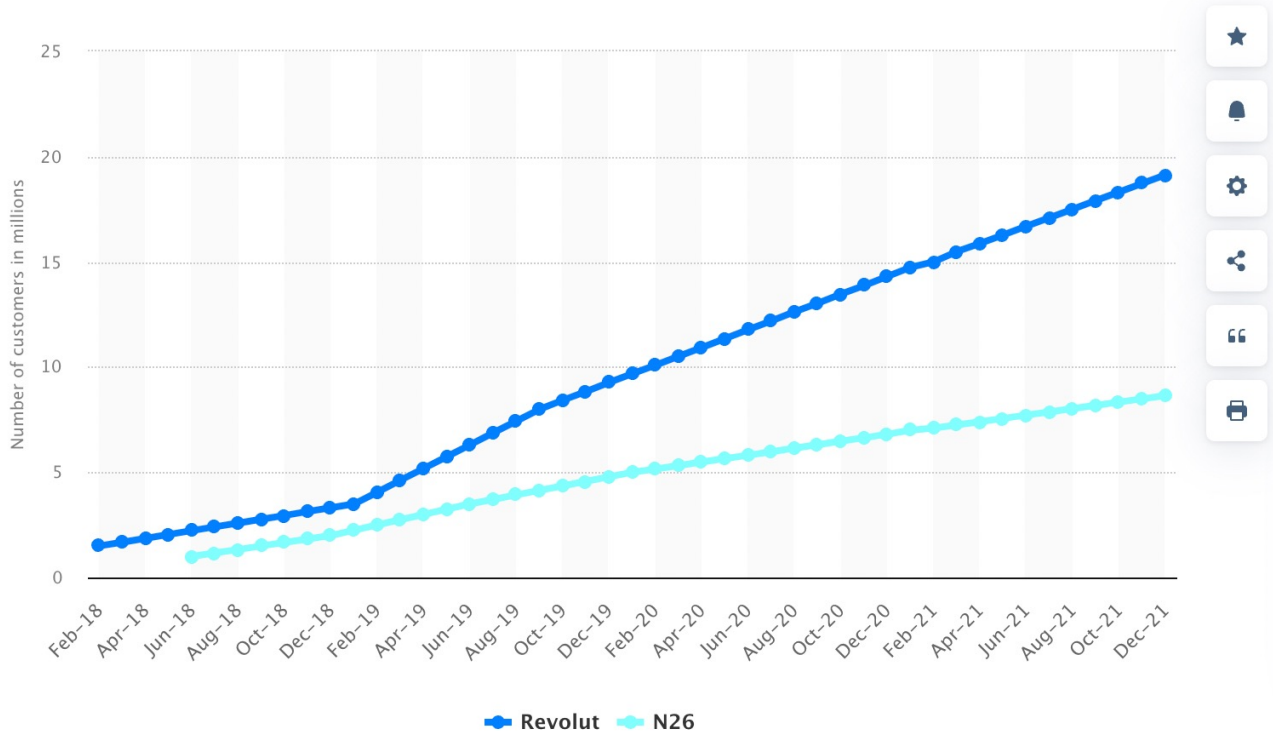
NeoBanks in EU

Finance & Insurance › Financial Services

PREMIUM +

Forecasted growth in customers of online only banks Revolut and N26 from 2018 to 2021

(in millions)



DOWNLOAD

PDF XLS PNG PPT

SOURCE DETAILS FAQ

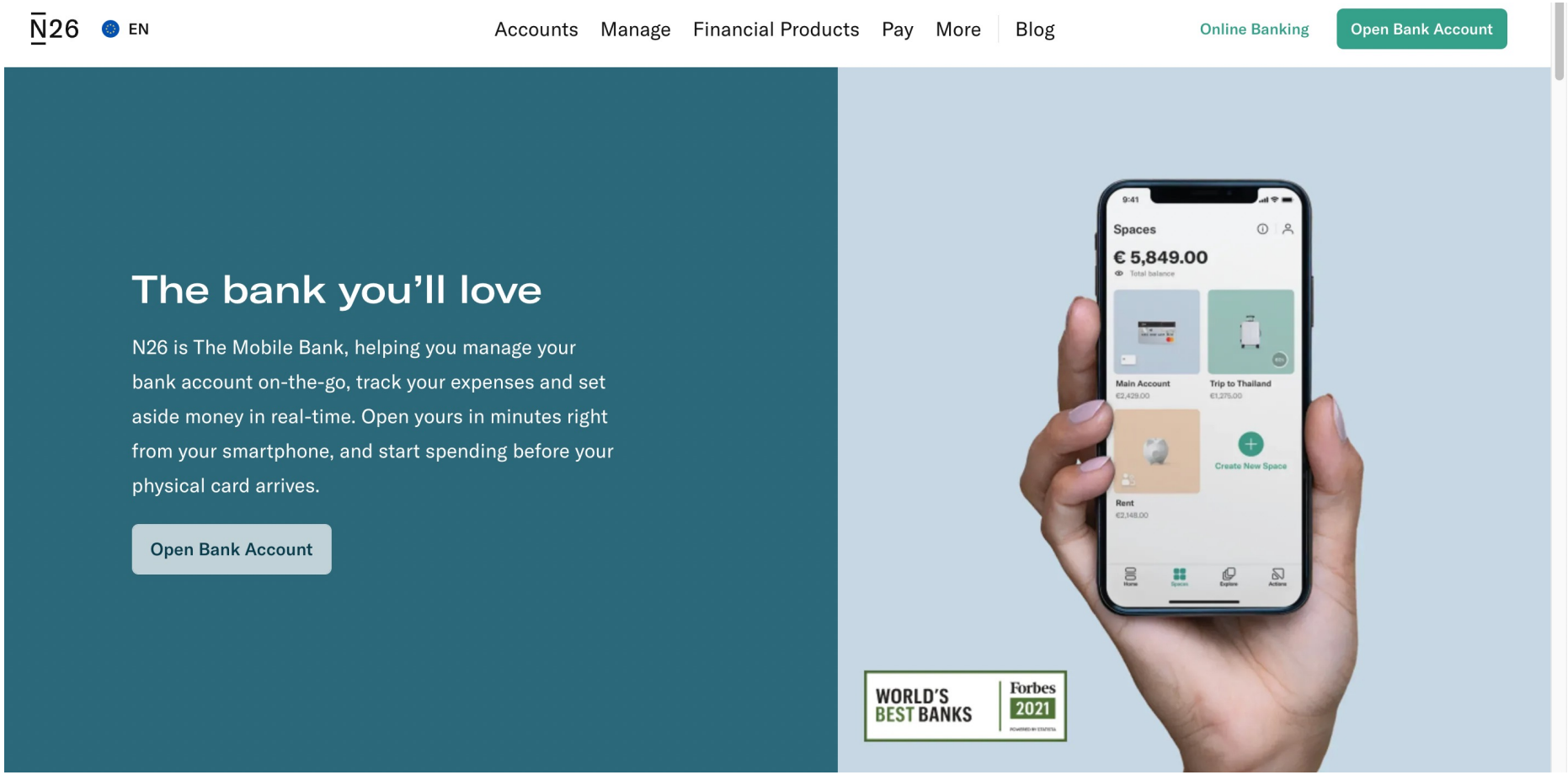
Sources
Various sources; Statista estimates

Survey by
Statista estimates

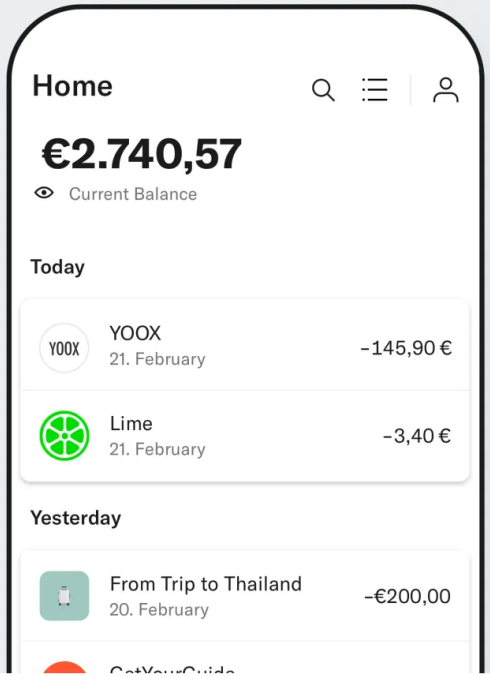
Published by
Statista estimates

Release date
2021

N26


N26
EN
Accounts
Manage
Financial Products
Pay
More
Blog
Online Banking
Open Bank Account
The bank you'll love
N26 is The Mobile Bank, helping you manage your bank account on-the-go, track your expenses and set aside money in real-time. Open yours in minutes right from your smartphone, and start spending before your physical card arrives.
Open Bank Account
Spaces
€ 5,849.00
Main Account
Trip to Thailand
Create New Space
Rent
WORLD'S BEST BANKS
Forbes
2021

N26



Your free N26 bank account

Get your free bank account in just 8 minutes and manage your money right from your smartphone. Discover smart features that give you more control over your finances. Get a virtual Mastercard right after opening your account—and connect it with Apple Pay or Google Pay to start spending right away.

Prefer a physical bank card? Order it for a one-time delivery fee.

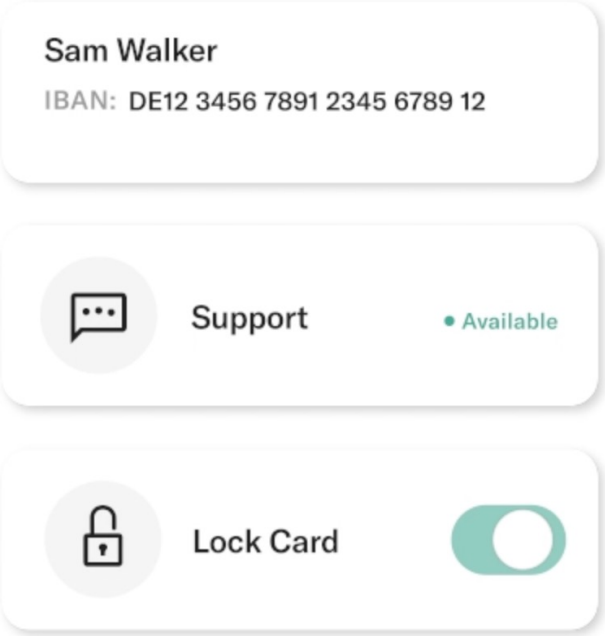
Open your free bank account >

N26

Security is a top priority at N26

N26 operates with a full German banking license, and your bank account with a German iBAN is protected up to €100,000, according to EU directives. And with fingerprint identification and advanced 3D Secure technology, you can rest assured you're extra safe when making purchases in stores and online.

Learn more about Security at N26 >

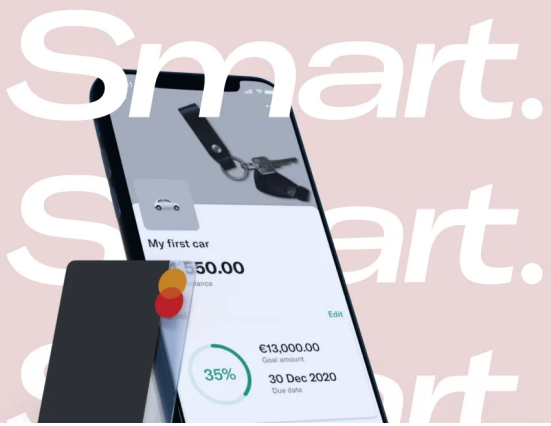


N26

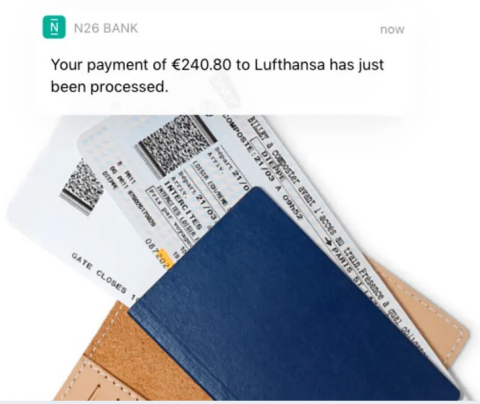
N26 Smart—save and spend with confidence

Discover N26 Smart, the bank account that gives you more control over your money—with a direct customer service hotline if you ever need support. Choose a Mastercard in your choice of 5 colors and organize your finances with 10 Spaces sub-accounts—including Shared Spaces to save together with others. Plus, get insights on your spending habits with Statistics, and learn to budget better along the way.

Get bank account >



N26



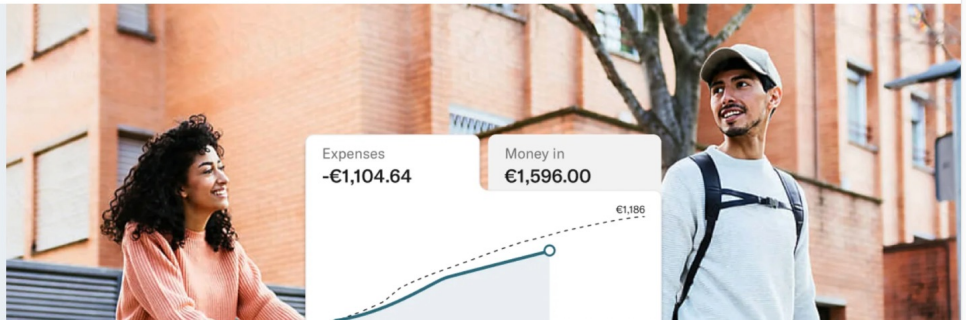
Stay tuned with push-notifications

Keep track of every transaction that comes in and out of your bank account, thanks to real-time push notifications. Whether you're withdrawing or depositing money, making a transfer or completing a monthly standing order—you're always kept up-to-date.

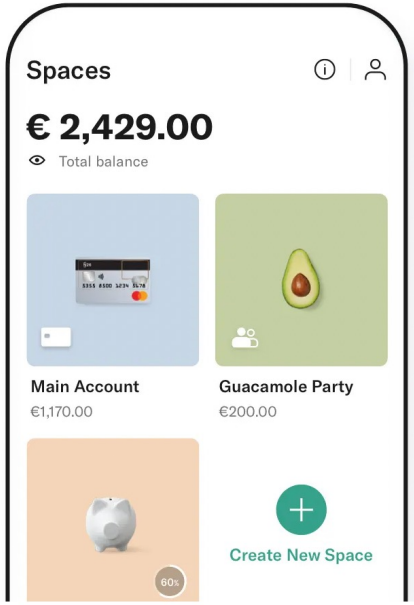
Open Bank Account

Get Insights into your spending habits

Not sure where all your money's going? Our Insights feature automatically categorizes your spending in real time. Track regular expenses, keep a pulse on your costs, and spot



N26



Reach your goals with N26 Spaces

Give your financial goals room to grow with N26 Spaces sub-accounts. Personalize each space with a name, set your savings target, and easily stash savings aside with just a few taps.

Rather set it and forget it? Easy—create Rules to regularly move money over to a space, or try Round-Ups to save up the spare change whenever you pay by card.

Manage Spaces sub-accounts >

N26 Support is here for you—in several languages.

If you have any questions or run into any problems, our N26 Customer Support team is always on hand to help you in English, French, German, Spanish and Italian. Just reach out to them via email or chat to an N26 expert right in your app.

N26

Key Partners

Back end infrastructure:

- Issuing and processing for payments: VISA (US) and Mastercard (EU)
- Banking back end infrastructure: Axos Bank (US) and Wirecard (EU)

Additional services:

- Moneybeam
- Transferwise
- Vaamo and others

Key Activities

- Cool and youth driven brand
- Agile and adaptive IT structure
- Partnerships

Key Resources

- Business expansion
- Customer centric product development
- Customer information analysis

Value Proposition

- Mobile bank account
- Business accounts for freelancers
- P2P Payments
- Low and transparent fees

N26

Customer Relationships

- Online and mobile customers
- Customer support team (over 600 employees)
- Customers feedback collection for company's improvement

Channels

- N26 App, website and social media page
- Partners' channels
- Brand ambassadors

Customer Segments

- Young customers (18-35 customers of retail banks)
- Freelancers and self-employed
- American users

Cost Structure

- IT infrastructure costs
- Marketing
- Administrative costs
- Regulatory costs

Revenue Streams

- Subscription based model
- Business accounts
- Usage fees

N26

Article • Banking

N26 customer growth limited by BaFin imposed customer cap

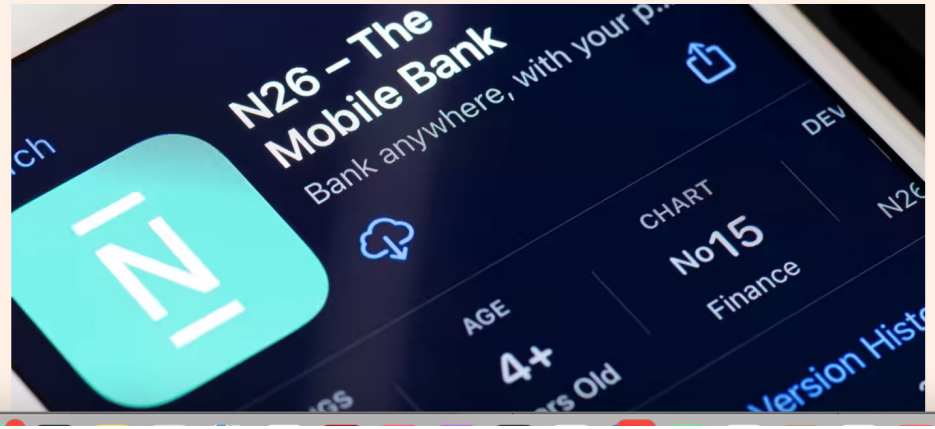
By Joanna England

October 19, 2021 • 5 mins

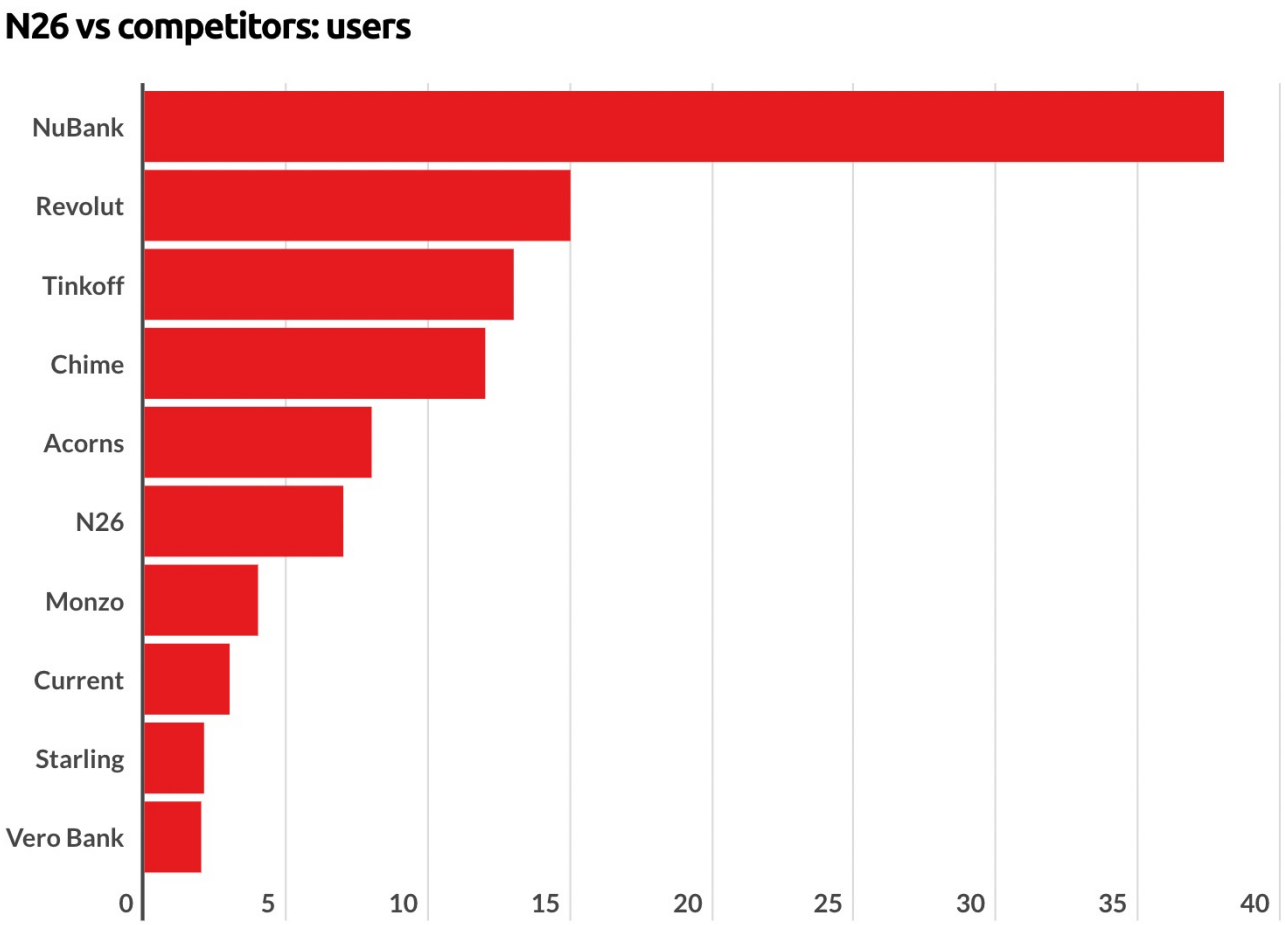
N26 + Add to myFT

Fintech N26 pulls out of US as it abandons global ambitions

Retreat follows last year's UK exit and series of public rebukes from German regulator



N26 vs World

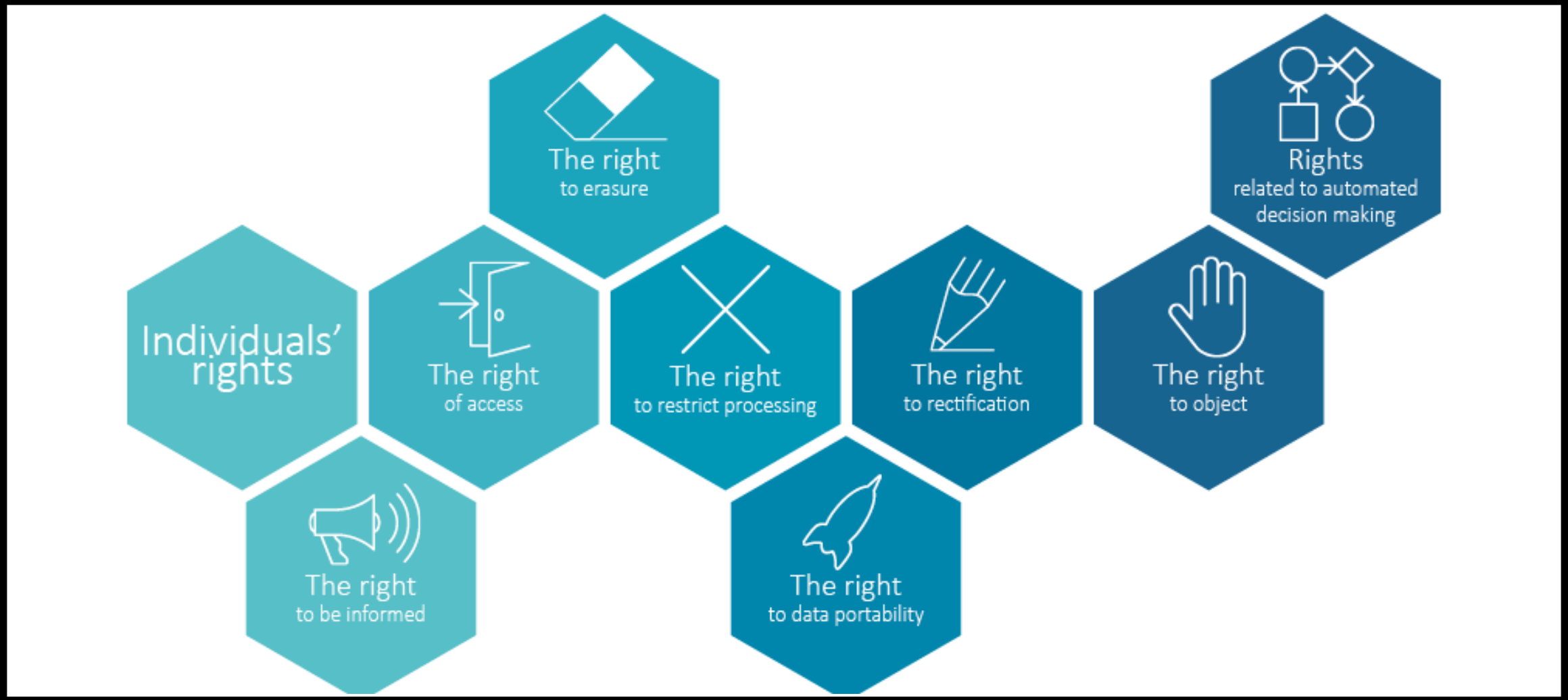


Sources: Company Data

Questions?

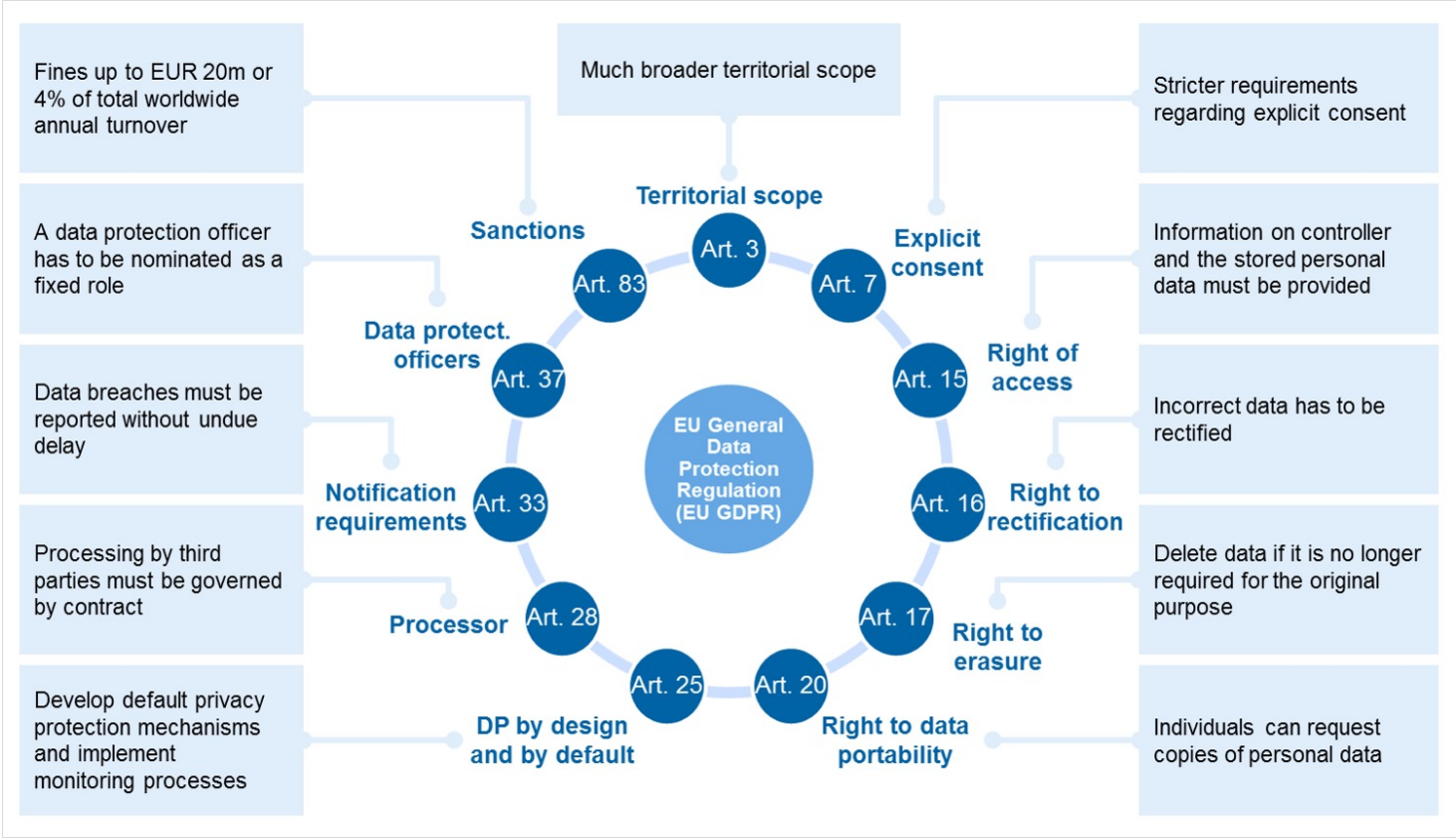
Privacy Law in the EU and the GDPR

--



The EU has a Comprehensive Privacy Regime—the GDPR

GDPR in EU


Fines up to EUR 20m or 4% of total worldwide annual turnover
Much broader territorial scope
Stricter requirements regarding explicit consent
A data protection officer has to be nominated as a fixed role
Information on controller and the stored personal data must be provided
Data breaches must be reported without undue delay
Incorrect data has to be rectified
Processing by third parties must be governed by contract
Delete data if it is no longer required for the original purpose
Develop default privacy protection mechanisms and implement monitoring processes
Individuals can request copies of personal data
Sanctions
Art. 83
Territorial scope
Art. 3
Explicit consent
Art. 7
Data protect. officers
Art. 37
Right of access
Art. 15
EU General Data Protection Regulation (EU GDPR)
Notification requirements
Art. 33
Art. 16
Right to rectification
Processor
Art. 28
Art. 17
Right to erasure
Art. 25
Art. 20
DP by design and by default
Right to data portability

Issue: GDPR and PSD2—Complementary or Conflicting?

Questions?

Underlying Legal Issues in US Consumer Financial Data Ecosystem

--

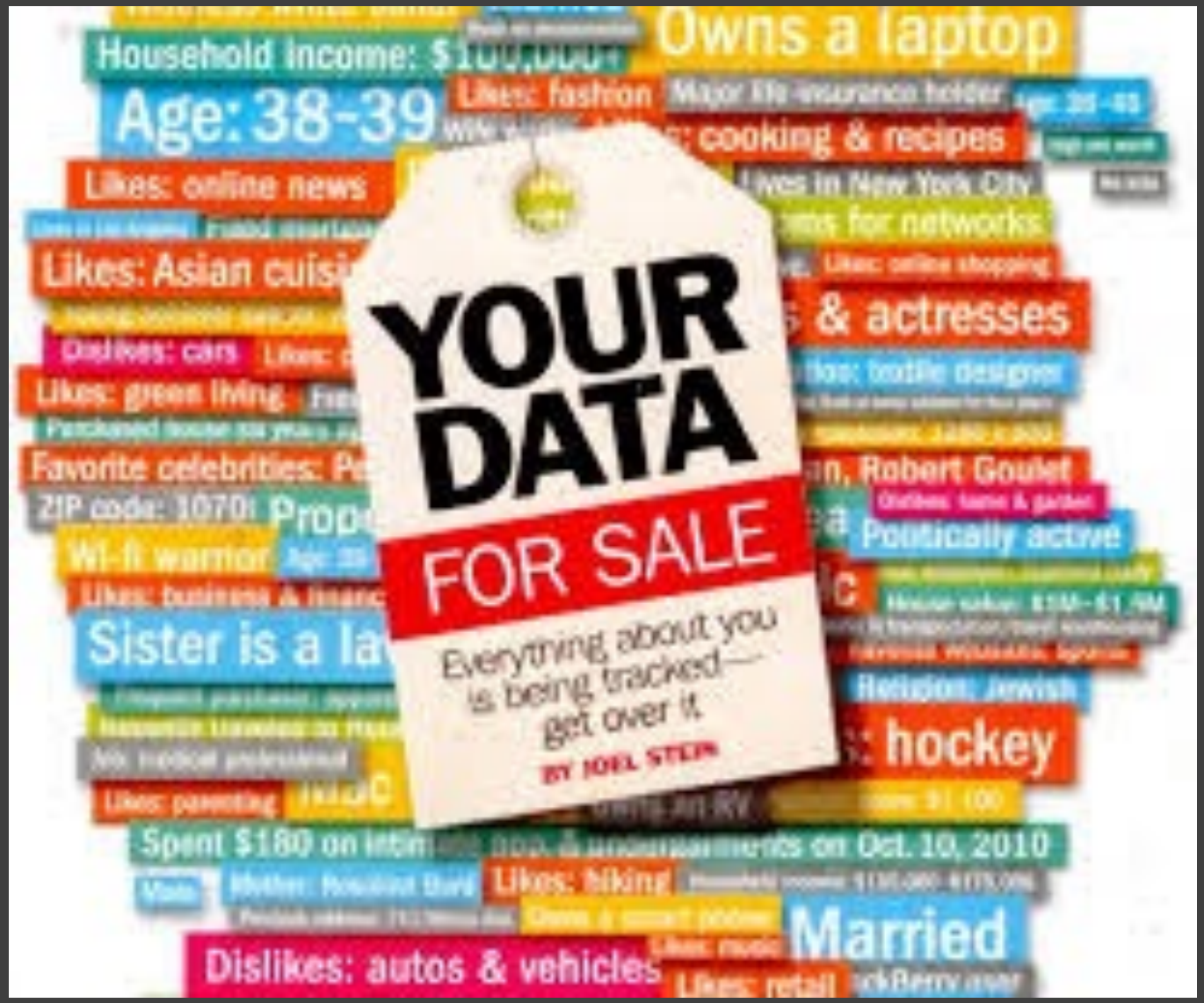
What Consumer Data are We Talking About? “Nonpublic Personal Information” or NPI

- The **Gramm-Leach-Bliley Act** Privacy Rule defines NPI as any **"personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available.””**
- **NPI is:**
  - ***any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);***
  - ***any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or***
  - ***any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).***
- **NPI does not include information that you have a reasonable basis to believe is lawfully made "publicly available."** In other words, that the information is generally made lawfully available to the public; and that the individual can direct that it not be made public and has not done so.
  - For example, while telephone numbers are listed in a public telephone directory, an individual can elect to have an unlisted number. In that case, her phone number would not be "publicly available."

Who Holds Personal Financial Data?

Who is Holding NPI?

- Personal financial data is stored in various formats in various places at banks, payments processors, insurance companies, broker-dealers, fintechs and their contractors (data aggregators).
- This data reflects transactions in the accounts of consumers at those institutions
- Historically, financial institutions made little use of their account data, but this has changed
- **Personal financial data also is held in enormous unregulated marketing company databases** and in the FCRA-regulated databases of credit bureaus



What Can Holders of Personal Financial Data Do With It?

Who Benefits From It?

Can Personal Financial Data be Property? Whose?

Andrew Yang View 1/2

"Each of us generates a significant amount of data each day during the normal course of our activities. Our phones and computers track our movement and actions, while our browsers and websites track our online activities. As we've seen, some of the largest tech companies can know more about us and our lives than our families and those closest to us.

As of now, that data is owned by the people who collect it, and they're allowed to do anything they want with it. They've sold it, used it to target us with advertisements, and have analyzed the vast quantity of data to draw conclusions on whole populations, allowing them to monetize it.

We've also seen it abused. Some companies haven't done enough to protect our data, resulting in breaches that have made our private information insecure. Others have sold it to disreputable companies, allowing them to target us for everything from marketing fraudulent services to influencing elections. Companies themselves have asked for better and clearer rules.

This needs to stop. Data generated by each individual needs to be owned by them, with certain rights conveyed that will allow them to know how it's used and protect it."

Andrew Yang View 2/2

"These rights include:

- **The right to be informed as to what data will be collected, and how it will be used**
- **The right to opt out of data collection or sharing**
- **The right to be told if a website has data on you, and what that data is**
- **The right to be forgotten; to have all data related to you deleted upon request**
- **The right to be informed if ownership of your data changes hands**
- **The right to be informed of any data breaches including your information in a timely manner**
- **The right to download all data in a standardized format to port to another platform**

Consent should be informed and active - companies are responsible for ensuring that they collect a positive opt-in from each user before collecting any data, and this opt-in should be accompanied by a clear and easy-to-understand statement about what data is being collected, and how it is going to be used.

You can waive these rights and opt in to sharing your data if you wish for the companies' benefit and your own convenience - but then you should receive a share of the economic value generated from your data."

Mark Jamison AEI View 1/2

One of the more curious proposals addressing online privacy concerns is for the government to award internet users ownership of information about their online activities. This online data property (ODP) idea has shown up in academic research and in Congress (for example here and here). **The gist of ODP is that when someone does something online, knowledge of that act becomes private property, and the person gains exclusive rights and control over it. So if I shop online for a new tie, I have exclusive rights and control over what others know about it.**

The ownership grant would apply only to online activities. If I shopped at a physical store for the new tie, the sales clerks can learn by observation and use that knowledge to help me and other customers in the future.

What is motivating this proposal? Apparently ODP supporters are responding to people's sentiments they interpret as violations of privacy. These sentiments could include fear that others see or know about him or her (scopophobia), fear of technology (technophobia), or fear of new situations (neophobia). My AEI colleague Jim Harper has pointed out that sometimes these sentiments are actually worries about fairness, security, intrusion, loss of autonomy, and objectification.

It is also possible that ODP supporters are simply attacking today's tech platforms for other reasons. But if the advocates are sincere, they rest on three myths.

- **Myth 1: Knowledge about someone is inherently his or her property**

Reality 1: Property ownership comes from creating, purchasing, or being gifted the property

We know that ODP assumes this myth because the proposals make no provision for compensating others when the law grants the internet user ownership. Rep. Doug Collins (R-GA) openly embraces the myth in his principles statement for ODP: "The data consumers generate needs to be recognized as their property — not someone else's."

How do we know Myth 1 is false? There are three reasons: (1) The idea is clearly incoherent for offline data, (2) online-offline is a false dichotomy for information, and (3) arbitrarily granting property rights conflicts with the workings of a market economy.

In the offline world, one plainly sees the incoherence of requiring that information about person A, written on paper by person B or stored in person B's mind, be controlled by person A: It gives person A control over person B's physical property and mind. A free society cannot function that way. But that will be the future under ODP as digitization erases the fabricated distinction between online and offline information.

The government cannot arbitrarily grant property rights and expect the economy to work. In an economy with private property, the proper methods for obtaining property rights are creating the property, purchasing it from its owner, or being gifted the property by its owner. Everything else is theft. Even copyright laws do not grant property rights for facts.

Mark Jamison AEI View 2/2

- **Myth 2: Tech companies unjustly take people's data**

Reality 2: Online services compensate people for revealing information about themselves

Following their embrace of Myth 1, ODP proponents conclude that tech companies' use of the data they gather is the moral equivalent of theft.

How do we know that the proponents are wrong other than the faulty premise of Myth 1? Since consumers are not purchasing data in ODP proposals, nor is it given to them, ODP proponents must believe the online user is the sole creator of knowledge when he or she acts online.

The proponents are wrong. Knowledge creation is joint work by the user and online platform: The platform creates an environment in which the user wants to act, the user acts, and the platform observes, records, and manages information on the user's actions. The platform does most of the work.

Not only that, economic studies find that platforms often compensate users for their online activities by providing discounted prices, including zero prices (see here and here). If ODP became law, there are two possible effects on this compensation. One possibility is that it would essentially stop, prices for online services would rise, and online experiences would decline in quality because platforms could not create services that target individual interests.

The other possibility is that, to comply with the new laws, online platforms would simply make the compensation explicit in their terms and conditions. In this case the user experiences with these platforms would likely be unaffected by the ODP law.

- **Myth 3: Given the opportunity, consumers will manage information about themselves**

Reality 3: Consumers find that the benefits of managing personal information are not worth the costs

Consumers rarely optimize their online privacy settings. It appears consumers' costs of learning about settings and adjusting them outweigh the negative sentiments that arise from letting platforms learn.

What does this tell us about how consumers would behave if they owned the online information about them? Most consumers would likely spend even less time managing personal data than they do managing privacy settings. This would likely result in: (1) some consumers never allowing access to the data, thus missing out on the benefits of personalized services, and (2) a third party emerging that would buy data property rights and become a data monopoly, which would then sell knowledge to platforms. It is hard to imagine scenarios in which these outcomes make consumers better off than the status quo.

ODP would also likely result in a decline in US online entrepreneurship. The costs of contracting with individual customers or a third-party data monopoly would be too great for many upstart online companies.

What should be done? Information should be treated as other types of property — namely, such that people can have exclusive rights and control of copies of information but not of the facts themselves. And the copies should be obtained the old-fashioned way: by buying them, receiving them as gifts, or creating them through mutually beneficial engagements between platforms and users.

Kerry and Morris/Brookings View

- Treating our data as our property has understandable appeal. It touches what the foundational privacy thinker Alan Westin identified as an essential aspect of privacy, a right "to control, edit, manage, and delete information about [individuals] and decide when, how, and to what extent information is communicated to others."
- It expresses the unfairness people feel about an asymmetrical marketplace in which we know little about the data we share but the companies that receive the data can profit by extracting marketable information.
- **The trouble is, it's not your data; it's not their data either.** Treating data like it is property fails to recognize either the value that varieties of personal information serve or the abiding interest that individuals have in their personal information even if they choose to "sell" it.
- **Data is not a commodity. It is information.** Any system of information rights—whether patents, copyrights, and other intellectual property, or privacy rights—presents some tension with strong interest in the free flow of information that is reflected by the First Amendment. **Our personal information is in demand precisely because it has value to others and to society across a myriad of uses.**
- **Treating personal information as property to be licensed or sold may induce people to trade away their privacy rights for very little value while injecting enormous friction into free flow of information. The better way to strengthen privacy is to ensure that individual privacy interests are respected as personal information flows to desirable uses, not to reduce personal data to a commodity.**

Questions?

Financial Data Privacy Law in the US

--

Many US Laws Already Apply to Consumer Financial Data

- Dodd-Frank Section 1033
- Gramm-Leach-Bliley Act (GLBA)
  - Privacy and Safeguards Rules
- UDAAP FTC/CFPB
- FFIEC Information Security Guidelines
- Third Party Risk Guidelines (FDIC, FRB, OCC)
- Regulation E/EFTA
- Fair Credit Reporting Act
- California Consumer Privacy Act of 2018 (amended 2020)

Some US Law Already Applies to Consumer Data-- Gramm-Leach-Bliley Act

- The Gramm-Leach-Bliley Act (GLBA) contains financial data privacy, including data security and data transmission rules. **There are two provisions that are relevant to the data sharing space: the "Safeguards Rule," which regulates data security, and the "Privacy Rule," which develops the boundaries of legal data sharing and the rights of consumers to receive notice and halt certain types of data sharing.**
- The GLBA states that the rules apply to "financial institutions," which are defined as any institution engaging in activities that a financial holding company may engage in. The FTC further interpreted the term "financial institution" to include any "institution that is significantly engaged in financial activities.

Some US Law Already Applies to Consumer Data-- Gramm-Leach-Bliley Act

- Under the GLBA's Privacy Rule, **"financial institutions" must provide a privacy notice to customers when a relationship with a customer commences and at least once a year thereafter.**
- These disclosures must include the policies and practices of the institution with regards to third-party data sharing of any type and the types of information that are collected by the institution. In 2009, eight federal agencies issued a GLBA "model form" for required privacy notices.
- **The GLBA also contains rules about third-party data sharing.**
- **The Act requires consumer notice and opt out for sharing any "nonpublic personal information" with an "affiliate" or "nonaffiliated third-party." This includes information shared with aggregators**.
- There are several exceptions to this rule, but the notice and opt-out regime is the default. **In addition, the third-party receiving the data cannot re-transmit the information unless that disclosure could have been lawfully made by the financial institution itself without a notice and opt out process with the consumer**.

FACTS	WHAT DOES CAPITAL ONE® DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: • Social Security number and income • Account balances and payment history • Account transactions and credit card or other debt

All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Capital One chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Capital One share?	Can you limit this sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	YES	NO
For our marketing purposes – to offer our products and services to you	YES	NO
For joint marketing with other financial companies	YES	NO
For our affiliates' everyday business purposes – information about your transactions and experiences	YES	NO
For our affiliates' everyday business purposes – information about your creditworthiness	YES	YES
For our affiliates to market to you	YES	YES
For nonaffiliates to market to you	YES	YES

To limit our sharing	Call us toll free at 1-888-817-2970 and one of our representatives will update your privacy choices. **Please note:** If you are a *new* customer, we can begin sharing your information 30 days from the date we sent this notice. If you're an *existing* customer and have opted out previously, you don't need to update your privacy choices again. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Go to capitalone.com/privacy or capitalone.com/contactus.

Please Recycle

Who we are	
Who is providing this notice?	Our affiliates include financial companies with the Capital One, Chevy Chase, Onyx, Paribus, and Greenpoint names, such as Capital One Bank (USA), National Association; and Capital One, National Association.
What we do	
How does Capital One protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
How does Capital One collectmy personal information?	We collect your personal information, for example, when you: • Open an account or depositmoney • Pay your bills or apply for a loan • Use your credit or debitcard We also collect your personal information from others, such as credit bureaus, affiliates, or othercompanies.
Why can't Ilimit all sharing?	Federal law gives you the right to limit only: • Sharing for affiliates' everyday business purposes – information about your creditworthiness • Affiliates from using your information to market to you • Sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. See below for more on your rights under state law.
What happens when I limit sharing for an account I hold jointly with someoneelse?	Your choices will apply to everyone on your account.
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. • *Our affiliates include financial companies with the Capital One, Chevy Chase, Onyx, Paribus, and Greenpoint names, such as Capital One Bank (USA), National Association; and Capital One, National Association.*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancialcompanies. • *Nonaffiliates we share with can include insurance companies, service providers, co-branded partners, retailers, data processors, and advertisers.*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. • *Our joint marketing partners include companies such as otherbanks and insurance companies.*

© 2017 Capital One. Capital One is a federally registered service mark.

Issue:Does FCRA Apply to Aggregators?

- **Are data aggregators consumer reporting agencies under FCRA?**
- Is a financial institution a data furnisher if it provides an API through which aggregators access data?
- “Some data aggregators, including Plaid, have argued that they [neither assemble or evaluate consumer reports] and merely function as a “pipe” for data... The Ninth Circuit found a similar argument persuasive in Zabriskie v. Federal National Mortgage Association, holding that Fannie Mae was not a consumer reporting agency because it merely provided a software tool that allowed mortgage lenders to assemble or evaluate consumer information themselves.”
- “On the other hand, a few aggregators, including Finicity, feel that their activities constitute more than functioning as a conduit and have already registered as consumer reporting agencies. Consumer groups argue that most, if not all, aggregators fall into this latter category and differences in the business models of Plaid and Finicity do not justify different treatment"
- https://projects.iq.harvard.edu/files/financialregulation/files/regulating_consumer_permissioned_access_to_financial_data_case_study.pdf

Some US Law Already Applies to Consumer Data-- FFIEC Information Security Guidelines

- Section 501(b) of **the GLB requires each FFIEC member agency to establish information security standards for those financial institutions under their jurisdiction** in order:
  - to insure the security and confidentiality of customer records and information;
  - to protect against any anticipated threats or hazards to the security or integrity of such records; and
  - to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Questions?

Privately Negotiated and/or Government Mandated Open Banking in the US?

--

Open Banking Access in the US is a Mix of Industry Politics, Regulators, Lobbyists, Contracts and Fears About Big Tech….

US Banks Prefer Contracts and Dedicated APIs

- **Large financial institutions tend to favor private contractual relationships over screen scraping and regulatory mandates**.
  - These bilateral contractual agreements use dedicated secure APIs to replace screen scraping.
  - The content of these contracts is private but likely solve the control issue and the security issue for banks by restricting allowable activities by aggregators and setting up systems to confirm the security capabilities of third parties.
- It is possible that **by signing such a contract, the aggregator becomes subject to a variety of legal restrictions on the use of the data it collects as a "contractor" to the bank**
- JPMorgan Chase, Wells Fargo, and Capital One have been the most active negotiating deals with aggregators to set up API linkages. These APIs give banks control over what data is shared and with whom. Recent contracts include:
  - Wells Fargo-Xero (June 2016)
  - JPMorgan-Intuit (Jan. 2017)
  - Wells Fargo-Intuit (Feb. 2017)
  - Wells Fargo-Finicity (Apr. 2017)
  - US Bank-MX, Finicity, Others (2019)

Industry Attempts to Standardize

FINANCIAL DATA EXCHANGE

ABOUT MEMBERSHIP

Home » About

About

The Financial Data Exchange (FDX) is a nonprofit organization that is dedicated to unifying the financial industry around a common, interoperable and royalty-free standard for the secure access of user permissioned financial data, aptly named the FDX API. FDX has an international membership that includes financial institutions, financial data aggregators, fintechs, payment networks, consumer groups, financial industry groups and utilities and other permissioned parties in the user permissioned financial data ecosystem.

FDX exists chiefly to promote, enhance and seek broad adoption of the FDX API technical standard and is dedicated to five core principles of user permissioned data sharing: Control, Access, Transparency, Traceability and Security.

The FDX board of directors includes organizations from across the financial ecosystem and all tiers of membership are given the opportunity to participate in the development, growth and industry acceptance of the FDX API and other objectives through FDX working groups.

FDX exists as an independent subsidiary under the umbrella of the Financial Services Information Sharing and Analysis Center (FS-ISAC), whose mission is to ensure resilience and continuity of the global financial services infrastructure.

See our **Frequently Asked Questions** for FDX US and FDX Canada for more information.

Big banks, aggregators launch group to hash out data-sharing issues

By Penny Crosman October 18, 2018, 9:00 a.m. EDT 5 Min Read

Several big banks, including JPMorgan Chase, Bank of America and Wells Fargo, have joined forces with data aggregators and fintechs to form a group designed to create a consistent standard for sharing customer information.

The Financial Data Exchange, launched Thursday, could mark a turning point in the battle between the various institutions over how to safeguard data yet at the same time allow access for legitimate purposes.

The goal is to create a standard that provides interoperability within the financial ecosystem in a way that maintains consumer control, security and choice.

TCH Model Bank/Aggregator Agreement

The Clearing House®

Home | About Us | RTP | Innovation | Connected Banking | Advocacy | Payment Systems | TCHPA | ECCHO | UID Lookup

Model Agreement

In order to enhance consumer control over the data they share with financial applications (apps) and to provide for a safer and more secure method to facilitate such sharing, The Clearing House Payments Company's (TCH) Connected Banking Initiative is focused on accelerating the ability of data providers, (e.g. banks) and data receivers, (e.g. data aggregators or fintechs) to establish safe and secure direct connections through application programming interfaces (or APIs). Unfortunately, legal agreements between banks and fintechs have sometimes taken 12 months or more to be developed and finalized and have become a significant bottleneck to API adoption.

In collaboration with its member banks and in consultation with fintechs, TCH has developed a **Model Agreement** that banks and data aggregators/fintechs can use as a reference to facilitate the development of API-related data sharing agreements. Use of the Model Agreement is entirely voluntary and the agreement is intended to be modified as circumstances may warrant. Further, the Model Agreement avoids taking any positions on commercial terms, which will need to be negotiated strictly between the parties. The Model Agreement does, however, provide a potential foundation of common, generally accepted terms that both parties can reference; reducing, if they choose, the need to define and negotiate the same terms each time they enter into a bilateral data access agreement.

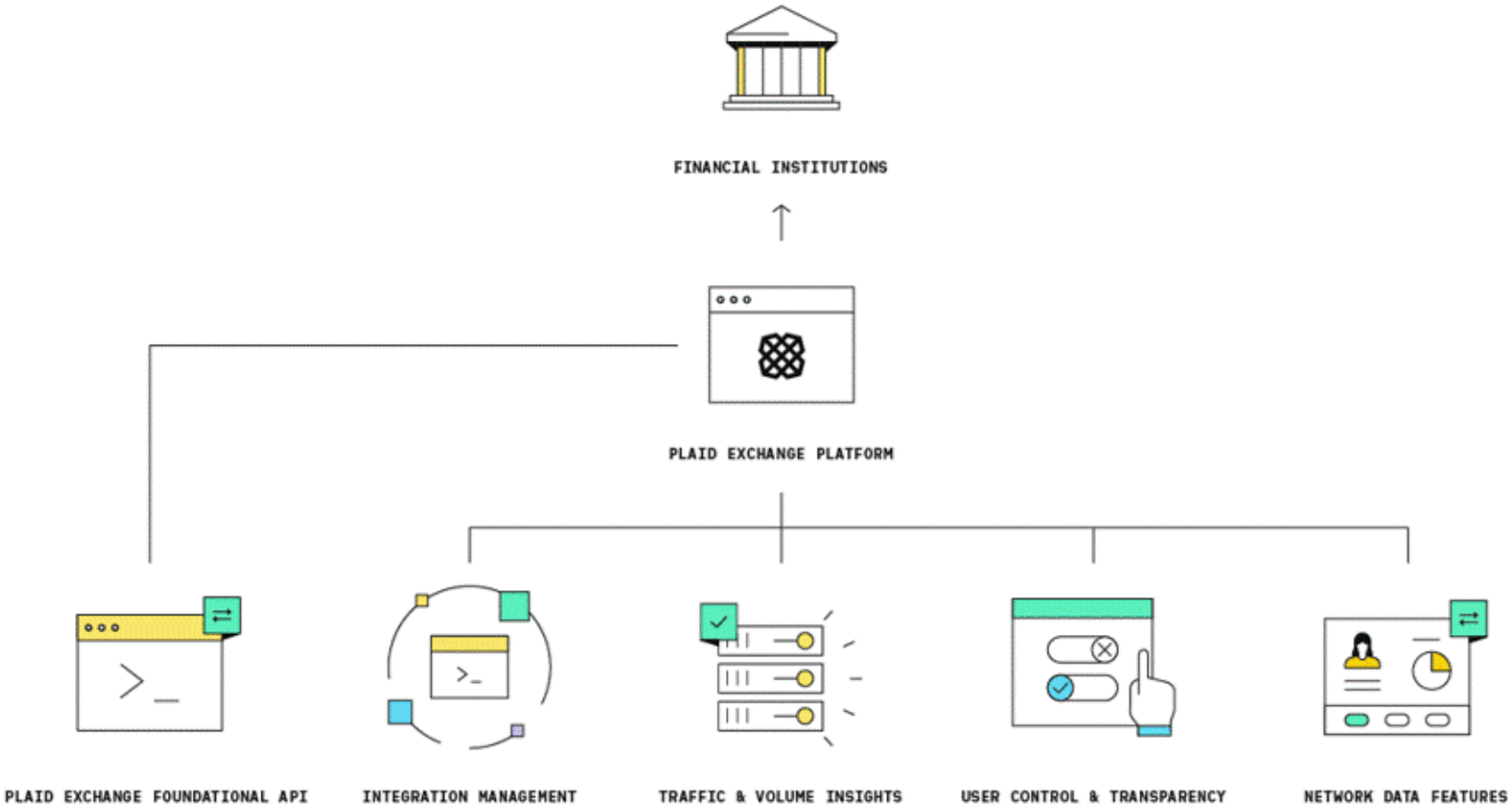
The Model Agreement has been specifically developed to be consistent with the CFPB's ***Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*** (Oct. 18, 2017). These principles focus on consumer control and transparency, safety and security of the data, and appropriate accountability for any risks introduced into the system. More information on how CFPB principles were incorporated into the Model Agreement is available **here**.

TCH has gone through significant effort to obtain feedback from multiple parties including banks, nonbank financial institutions, and fintechs. The Model Agreement, however, is intended to be a living document, subject to continued modifications and updates that may reflect evolutions in technology and other factors. We encourage feedback that may be useful to improve future versions.

Please send any feedback **here**.

Download the Model Agreement

Aggregators Have Worked to Create Open API Platforms



Incumbents are Reluctantly Making it Work in US

DATA SHARING

BofA, Chase, Wells Fargo pilot service to rein in screen scraping

By Penny Crosman January 26, 2021, 1:10 p.m. EST 4 Min Read

A new type of vendor service aims to make life easier for bankers who want to assess the risks of working with certain data aggregators.

Several large banks, including Bank of America and JPMorgan Chase, have recently piloted the Streamlined Data Sharing Risk Assessment offered by The Clearing House and the risk-assessment providers TruSight and KY3P. The two companies collect responses from aggregators to hundreds of questions and review their internal documents as well as conduct on-site visits.

But Law Might Intervene: Dodd-Frank Section 1033

- In the Dodd-Frank Act of 2010, Congress gave express authority to the CFPB to regulate consumer financial information
  - "Subject to rules prescribed by the Bureau, a covered person **shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers**."
  - ***Is this self-executing?***

CFPB Has Finally Commenced 1033 Rulemaking

1033 ANPR Questions

- **The ANPR contains a series of questions on which the Bureau seeks comment. The questions are grouped into the following nine topics:**
  - **Benefits and costs of consumer data access**
  - **Competitive incentives and authorized data access**
  - **Standard-setting**
  - **Access scope**
  - **Consumer control and privacy**
  - **Legal requirements other than section 1033**
  - **Data security**
  - **Data accuracy**
  - **Other information**

FEBRUARY 05, 2021

Plaid's comments to the CFPB on Dodd-Frank 1033

Ben White & Katie Neal

Last October, we wrote "A call to action for fintech," to highlight the Consumer Financial Protection Bureau's (CFPB) opportunity to set the stage for the future of financial services by empowering consumers with stronger data rights.

Since then, Plaid has worked with our stakeholders - fintech companies, financial institutions, and, above all, consumers - to build our case for the CFPB to take action to ensure consumers can control their data in order to benefit from fintech. These efforts ultimately led to our submitting a comment letter in response to the CFPB's Advanced Notice of Proposed Rulemaking on Consumer Access to Financial Records, which addressed Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

In our 50+ page comment letter, Plaid laid out our view of the current market, and our vision of the future of consumer control of their data. We also brought together a group of fintech companies to submit a coalition letter.

Here's what Plaid asked the CFPB to consider in its rulemaking:

- **Enforce consumer rights to authorized data access:** Consumers rely on their ability to authorize third parties' access to their financial information in order to power fintech products and services that help them improve their lives. To ensure that all consumers enjoy consistent authorized access to their financial information, the Bureau should establish rules enforcing broad Section 1033 rights.
- **Supervise data aggregators:** Data aggregators play a critical role in the authorized data ecosystem by acting as consumers' agents and carrying out consumer desires to share data. Many data aggregators, including Plaid, have reached a size at which supervision would provide helpful oversight and assurances to the financial data ecosystem.
- **Don't mandate technologies:** Collaborative, industry-led standards-setting is underway. The Bureau should establish principles-based guidelines for these standards to meet, so that standards can satisfy consumer expectations and evolve with technological innovation.
- **Monitor practices to ensure competitive incentives do not impact consumer access:** Competitive incentives in the authorized access ecosystem will grow as data holders become data users and vice versa. The Bureau should prevent data holders from restricting consumer data access to further their competitive interests.
- **Assess ecosystem readiness:** To ensure that consumers at all data holders have equal access to the fintech ecosystem, the Bureau should regularly assess the availability and consistency of authorized access.

Each of these recommendations rolls up into our broader view of what the future of financial services looks like: consumers at the center, free to take their data with them to any provider that meets their needs.

We believe that this framework would enable the CFPB to ensure that consumers have all the protections they need, and that innovators can continue to build on the promise of fintech.

National Consumer Law Center Comments

- The potential benefits for consumers of authorized data access, assuming strong provisions for consumer control, security, and use limitations, are significant, as consumer use of their own data could provide a better alternative and provide true competition to the Big Three credit bureaus**. The CFPB should issue a strong rule under 1033 to ensure protections for consumers accessing their own account data.**
- Authorized data access also poses significant risks to consumers. Consumers face the dangers of losing control over the data, having it used against them, and having their privacy invaded. **The type of consent currently obtained by data aggregators and the lack of limits on use of that data leave consumers vulnerable to abuse, exploitation, and security risks.** The CFPB must issue strong rules mandating true consumer control over their own data, substantive limits on how companies can use and share data, and **meaningful choice** over whether consumers want to share that data.
- The CFPB should encourage aggregators to move away from screen scraping and should encourage financial institutions to accept data sharing through application programming interfaces (APIs), but the Bureau cannot prohibit screen scraping until all consumers at any financial institution have the ability to access their own data through APIs**. The CFPB should set broad-based standards for authorized data access, such as a common data dictionary, or require the establishment of industry-wide standards**. The CFPB should ensure data security through supervision of data aggregators and data users; also, aggregators should be governed by the FTC Safeguards Rule issued under Gramm-Leach-Bliley Act.
- The CFPB should guarantee that consumers are protected when their account data is accessed and used by companies**. It should exercise supervisory authority over data aggregators**, and ensure application of strong protections under the Electronic Funds Transfer Act, Equal Credit Opportunity Act, and the Fair Credit Reporting Act.
- The CFPB should adopt rules under Section 1033 to give consumers the **right to information beyond deposit account data, such as: (a) a copy of the consumer report or risk score that a covered person used in connection with providing the consumer a financial product or service; (b) records retained by a covered person pursuant to Regulation Z or Regulation B; and (c) behavioral data sold by the credit bureaus to covered persons for marketing purposes.**
- Finally, NCLC has written extensively on the risks involved with the use of the financial account transaction data for which they authorize access, and the guardrails that are necessary to ensure that consumers benefit and are not harmed by such use.

American Financial Services Ass'n.

- Section 1033(a) provides that, subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, certain financial data. The Bureau should note that all consumers with internet access now have access to their financial data that is with a financial institution with an online platform. A proposed Section 1033 rulemaking arises because the Consumer Financial Act of 2020 defines "consumer" so very broadly that term includes an "agent, trustee, or representative acting on behalf of an individual."4 Section 1033(b) then outlines certain broad exceptions from these general access rights.
- The exceptions under 1033(b) include:
  - any confidential commercial information, including an algorithm used to derive credit scores or other risk
  - scores or predictors;
  - any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;
  - any information required to be kept confidential by any other provision of law; or
  - any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.
- In the plethora of written material regarding Section 1033, the discussion of 1033(b) is surprisingly limited. We hope this is because the exemptions are clear and transparent and little interpretation is needed. AFSA believes that this subsection is crucial to implementing Section 1033 in a manner that ensures the protection of consumers' data. For years there has been a trend in regulation at the international, national, and state levels to better protect consumers' data. **AFSA members have spent incredible amounts of time and money enhancing their data protection systems. It seems contrary for a regulation to reverse that trend and require financial institutions to share consumers' data in a manner that puts that data at greater risk of a breach.**
- Providing consumer data to third parties, such as aggregators, puts that data and hence financial institutions, at considerable risk. Financial institutions are already at risk of having their customer data hacked and sanctioning the opening of that data to aggregators will necessarily heighten that risk. Financial institutions may not be able to perform adequate risk assessments of unregulated third-party data aggregators and should not be burdened with the extraordinary expense of doing so. **Section 1033(b) provides a way for financial institutions to manage that risk because it clearly allows them to refuse to provide third parties with access to customer non-public personal information (NPI).**
- AFSA strongly supports the Bureau implementing rules that construe Section 1033(b) broadly as the statutory language demands. A broad interpretation of Section 1033(b) will allow financial institutions to better protect their customers' data and still comply with the myriad of federal and state privacy laws. Broad exemption authority under Section 1033(b) will not prevent consumers from accessing their own data because they can always directly access their own data; however, it will limit the access of data aggregators to that data, and, in turn, better protect the data. Consumer cannot have privacy unless their data is secured.
- **Thus, AFSA recommends the Bureau give financial institutions clear authority to decline to share with data aggregators under Section 1033(b). In addition, we recommend the Bureau address section 1033(b)(3) as it relates to exceptions of "any information required to be kept confidential by any other provision of law." Specifically, "any other provision of law" should be defined so it includes both federal and state laws as well as any developed common law.**
- **Furthermore, we suggest that that to establish clear consumer control, consent, and disclosure, the Bureau: (a) allow financial institutions to require that their customers consent to data sharing with a third party annually (an opt-in as opposed to an opt-out); (b) have an easy opt-out of any data sharing at any time; and (c) require the data aggregator to disclose to the consumer what data it is gathering and how it will use that data, so aggregators will not use consumers' data in a manner they never contemplated. AFSA is concerned that, without controls, consumers will not understand how their data is being used and by whom. Allowing for annual consents and opt-outs preserves some level of control for consumers.**

Bank Policy Institute Comments

BANK POLICY INSTITUTE

- Coordination with Other Regulators. As an initial principle, it is important for the CFPB to coordinate its efforts to implement Section 1033 with the other prudential regulators, as well as the Federal Trade Commission, given that the CFPB's primary authorities do not extend over all operational risks related to such data sharing….
- Sufficient Flexibility and Innovation in the Marketplace. The CFPB's efforts to set standards for consumer authorized data sharing should ensure sufficient flexibility and innovation in the marketplace. The financial services industry continues to collaborate to develop technical solutions that enable consumer access to financial data while ensuring appropriate consumer protections. These efforts include the development of common technical standards for the secure access of consumer-permissioned data. **BPI believes that industry-led standards setting bodies are best positioned to unify the financial industry around common and interoperable technical standards while ensuring continued innovation and competition throughout the marketplace. The CFPB should encourage market-driven solutions and avoid engaging in specific technical standard setting for consumer data sharing.**
- Comprehensive Approach to Consumer Privacy and Transparency. Ensuring consumer privacy and transparency in how data is accessed, shared, and maintained should be central to the CFPB's process under Section 1033. **The CFPB should clarify that the GLBA would apply to data aggregators and other authorized entities to ensure the appropriate consumer privacy standards and leverage existing GLBA disclosure obligations in place to protect customer information.** The CFPB also should consider ways to improve the transparency of the consumer consent process, which would provide consumers with more awareness and control over their financial data. Additionally, the **CFPB should consider promulgating specific disclosure requirements under Section 1032 of the Dodd-Frank Act, ensuring that data aggregators provide consumers with the information needed to make responsible decisions about the sharing of their information**.
- Consistent Safeguarding of Consumer Data. **The CFPB should ensure that data aggregators appropriately safeguard consumer data in a manner commensurate with the legal obligations placed on banks. The CFPB should clarify that GLBA applies to data aggregators for the purposes of consumer data security, and coordinate with the FTC to expand the Safeguards Rule to expressly address data aggregators' security practices. The CFPB should consider designating data aggregators as larger participants of the consumer financial data services marketplace, providing direct oversight over data aggregators through regular supervision and examination.** The CFPB should also clarify the rights of consumers and the allocation of liability based on how the data flows between permissioned entities, beginning with clarifying liability for unauthorized transactions under Regulation

FTC

September 29, 2020

FTC Holds Workshop on Data Portability

LinkedIn Facebook Twitter Send Embed

Ballard Spahr

CyberAdviser
Insights from the frontlines of privacy and data security law

On September 22nd, the Federal Trade Commission (FTC) hosted an event, "Data To Go: An FTC Workshop on Data Portability," to examine the potential benefits and challenges to consumers and competition raised by data portability. Data portability means giving consumers the ability to receive a copy of their data for their own use or and move the data to another entity or service.

The workshop did not focus on any specific policy proposals or legislation, but the FTC expressed a desire to begin discussions as issues associated with data portability continue to evolve. The FTC noted that in addition to providing benefits to consumers, data portability may benefit competition by allowing new entrants to access data they otherwise would not have so that they can grow competing platforms and services. At the same time, the FTC recognizes that there may be challenges to implementing or requiring data portability.

During the workshop, FTC staff discussed several examples of existing data portability laws and regulations, such as the right to data portability under Article 20 of the European Union's General Data Protection Regulation (GDPR) and the right for consumers to make requests for portable data under the California Consumer Privacy Act (CCPA). The FTC noted that other countries have taken different approaches, like India and the United Kingdom's data portability regulations that are narrowly tailored to address only the health and financial services sectors

WRITTEN BY:

Ballard Spahr LLP
Contact + Follow

Katie Morehead + Follow

Kim Phan + Follow

PUBLISHED IN:

California Consumer Privacy Act (CCPA) + Follow

Consumer Financial Protection Bureau (CFPB) + Follow

Consumer Privacy Rights + Follow

Cybersecurity + Follow

Data Security + Follow

Data Transfers + Follow

Dodd-Frank + Follow

Financial Services Industry + Follow

FTC + Follow

Biden Administration

THE WHITE HOUSE

Administration Priorities COVID Plan Briefing Room Español MENU

BRIEFING ROOM

Executive Order on Promoting Competition in the American Economy

JULY 09, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote the interests of American workers, businesses, and consumers, it is hereby ordered as follows:

Toggle Large Font

- **Financial Data Portability (CFPB).** The Director of the Consumer Financial Protection Bureau (CFPB) is "encouraged to consider" rulemaking under the Section 1033 of the Dodd-Frank Act to "facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products." Sec. 5(t). The CFPB has been engaged since at least 2020 in rulemaking under Section 1033 with respect to consumer access to financial records. Similar approaches to Open Banking and the role of data portability are currently advancing also in the EU, with the PSD2 Directive, and in India. Of note, the FTC has already been exploring the benefits and challenges of data portability more broadly for consumers and competition.

New Sheriff in Town

The Senate confirmed Rohit Chopra to be director of the CFPB.

Photographer: Alex Edelman/Bloomberg

Chopra to Tackle Stacked CFPB Agenda After Winning Confirmation

BUSINESS

Senate confirms Rohit Chopra to lead the Consumer Financial Protection Bureau

October 1, 2021 · 10:45 AM ET

THE ASSOCIATED PRESS

Questions?

A Natural Experiment?

- Clear differences in regulatory approach between the US and the Eu
- What conclusions do you draw from those differences?

Is One Approach Working Better?

THERE ARE NOW **5 MILLION USERS** OF EU OPEN BANKING IN A POPULATION OF NEARLY 450 MILLION PEOPLE, AND **80 MILLION USERS** OF US OPEN FINANCE IN A POPULATION OF 330 MILLION PEOPLE.

WHY IS THIS?

"EU OPEN BANKING IS BASED ON THE FLAWED PREMISE THAT BANK CUSTOMERS WANT TO UNLOCK THE VALUE IN THEIR BANKING DATA. ON THE OTHER HAND, US OPEN FINANCE IS BASED ON THE VALID PREMISE THAT BANK CUSTOMERS HAVE UNMET FINANCIAL NEEDS THAT HAPPEN TO WANT THEIR BANKING DATA." (KATHARAMAN SWAMINATHUN)

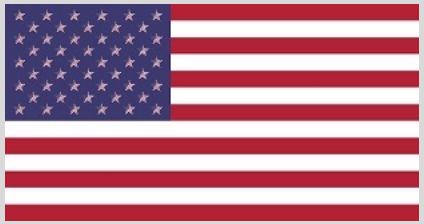
Proactive vs. Reactive?

- **EU is Proactive**
- "Open Banking in EU and UK may have started, principally, as way to promote competition in the payments and banking industry. But it is clear now that its impact is much broader.
- Open Banking promises to create a new data sharing infrastructure, which will form the basis of a much richer range of services and products across the whole of financial services, and critically, in other industries as well." (Deloitte)
- **US is Reactive**
- "The US have…opted for a market-led approach, but without any material government initiatives to support the development of Open Banking products and services….[D]ue to the highly fragmented and state-based nature of banking and banking regulation in the US, as well as a cultural aversion to 'red tape', there is little discernible appetite currently for taking this forward and issuing a common federal policy on Open Banking." (Deloitte)

Questions?

Do Styles of Regulation in EU and US Differ?

- Expert Driven
- Implemented Through Legislation
- Industrial Policy-Driven
- Anti-Monopoly
- Consumer Consent
- Level Playing Field
- Core Values?



- Politically Driven
- Implemented Through Regulation
- Market-Driven
- Preserves Oligopoly
- Consumer Consent
- Uneven Playing Field
- Core Values?