Vanta

EBOOK

Fortifying Fintech:

Security must-haves for Europe's trailblazers

Table of contents

Introduction: Trust – a key value-driver for fintechs

The security landscape is hugely challenging right now, with 55% of businesses saying security risks for their organisation have never been higher. This is a concern for all types of organisations – but especially for fintechs who deliver high-stakes banking and financial services.

Security is a non-negotiable for fintech companies and the sensitive information they handle. With fintech companies growing in popularity, the sector is becoming a bigger target for cyber criminals. Last year, cases of identity fraud within the fintech sector grew by 156% year-on-year with relatively new technologies such as AI driving the level of risk up even further.

But in addition to more pressure, an increasingly complicated risk landscape can bring more opportunities. Fintech is one of the fastest growing business and investment areas with over 9,000 companies in Europe alone. To stand out in such a crowded marketplace every organisation must use what's in its power – including security posture – to develop its competitive edge. One of the ways fintechs are doing this is by demonstrating trust.

Customers want to be assured that their sensitive data remains safe and for fintechs security is tied to success. The emphasis is therefore on companies to deepen the level of trust with their customers and go beyond the standard when demonstrating compliance. So how can fintechs keep up and ensure they are not compromising security and trust for innovation?

In this guide, we'll explore the biggest trends and challenges that fintech companies face, how they can streamline security and why good security means good business.

Security matters — whatever the fintech

Fintechs are responsible for increasing amounts of sensitive information including personal details, banking information, transaction history and more. The result has been rapidly evolving standards, best practices and regulations— including ISO 27001, SOC 2, PCI DSS, and DORA — with non-compliance with the latter costing organisations up to 2% of their global annual turnover or €10 million (whichever is higher).

Contributing to this is the fact that many fintechs must be "born global" to reach international markets and achieve rapid growth. This requires them to scale internationally quickly from day one. But while this approach brings additional revenue streams, it also brings additional risks and requirements.

For fintech companies, security and compliance matters more than ever. But depending on the type of fintech, it can have additional hidden risks — and potential opportunities. Let's take a closer look.

Business model

Fintechs traditionally fall into two types of business models — B2B and B2C. And for each, there are multiple motivations when it comes to demonstrating trust.

B2B - Data protection, competitive difference, reputation.

B2C - Fraud prevention, customer data security, incident response.

Type of fintech

There are also many different types of fintech with different security motivations and obligations:

Payments

- Security motivations: Payment companies must assure their customers that credit card data is secure and that they are protected against financial crimes.
- **Compliance obligations:** PCI-DSS compliance, fraud detection, compliance with anti-money laundering (AML) regulations.

Insurtech

- **Security motivations:** Peace of mind is paramount for insurtechs, and companies need to guarantee the safety of all sensitive customer data — from personal to financial to medical information.
- **Compliance obligations:** Claims fraud detection, insurance regulations, GDPR.

Consumer and business banking

Security motivations: Banking fintechs are major targets for cyber attacks and they must work hard to demonstrate trust to banks and consumers when it comes to protecting their funds.

Compliance obligations: Secure online banking, compliance with financial regulations, GDPR.

Financial operations (FinOps)

Security motivations: In addition to fraud prevention, FinOps companies must safeguard data integrity (especially in reporting) that is protected from leaks and manipulation.

Compliance obligations: Secure financial transactions, SOX ITGC controls to ensure compliance with the Sarbanes-Oxley Act.

Wealth management

Security motivations: High-wealth clients often demand clearer proof of authentication and security measures, while customer assets can range from real estate, to private funds, crypto and more.

Compliance obligations: Client data protection, GDPR.

Trading

Security motivations: Trading fintechs must balance real-time transactions with security, and protect traders against any abuse of the trading system.

Compliance obligations: Preventing market fraud and Distributed Denial-of-Service (DDoS), compliance with MiFID II.

Lending

Security motivations: Lending companies must provide a frictionless lending experience to customers and ensure they are resilient to fake identities or loan stacking.

Compliance obligations: Loan fraud prevention, risk assessment.

Spend management

Security motivations: Spend management customers will want assurances that their financial data is secure from unauthorised access, including fraudulent expense claims, while also having flexible employee controls and access.

Compliance obligations: Expense fraud detection, PCI-DSS compliance to secure company credit card data.

Crypto

Security motivations: Crypto companies must respect customer anonymity while also protecting them against DeFi (decentralised finance) vulnerabilities.

Compliance obligations: Wallet and private key protection, evolving compliance including anti-money laundering (AML) and know your customer (KYC).

Despite the many ways fintechs differ, one thing connects them — security and compliance frameworks. Read on to discover the key associated challenges facing fintechs in Europe, and how companies can manage multiple frameworks without multiplying the work.

The key challenges facing fintechs in Europe

Fintechs aren't short of challenges – after all a rapidly growing sector faces rapidly growing expectations. Today, the average fintech customer doesn't just expect advanced financial technology and innovative solutions, but a premium experience that keeps their most sensitive data safe.

Customer trust is therefore a major value-driver for fintech companies. But it is also a moving target. To this end, below we explore the three main obstacles preventing organisations from hitting it.

Challenge #1

Growing compliance requirements

The growing list of industry standards, best practices and regulations means fintechs are spending more time adhering to security and compliance frameworks – whether it's ISO 27001, SOC 2, DORA, PCI DSS, or all of the above. In turn, this means fintech companies are spending hours completing activities such as security questionnaires – all manually.

The result is not just lost time, but lost security and innovation. When multiple hours are spent on manual compliance tasks, the security team's time is redirected from other large-scale challenges such as fraud and AML, and ensuring their security posture scales with new geographics and new products and features. More generally, for fintechs, innovation is fuel, and the reason payment, insurtech and other fintechs stand out in such competitive spaces is down to their ability to innovate. But when time is spent on manual work, businesses operate inefficiently and end up losing ground to the competition.

11 working weeks a year are spent on manual compliance.

Challenge #2

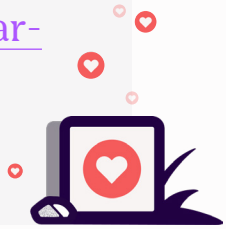
Protecting (and demonstrating) trust

The risk of cyberattacks and data breaches is only growing. For fintechs and the amount of sensitive data they handle, this can have a significant impact on customer and partner trust. Without customer trust, fintechs experience lost revenue and increased customer churn.

This is because the security expectations of customers have never been higher and whether a company deals with wealth management, loans or crypto, these are areas where customers require demonstration of compliance and seek assurances over their financial information. Banks for instance – at a 46% rate when compared to other sectors – are most frequently affected by cyberattacks.

Some early-stage startups might choose to gamble with deprioritising compliance until they're asked for it as part of a deal. But for fintechs, compliance – and demonstrating trust – is non-negotiable from day one. And, once it's lost, trust is hard to get back – especially as the wounds from reputational damage and lost investor confidence run deep.

48% of businesses believe good security practices drive customer trust for their business – a year-on-year increase of 7%



Challenge #3

Growing compliance requirements

Depending on the size of their business, fintechs might rely on third-party vendors for a variety of services – from payment processing to data analytics to fraud detection. But these relationships require them to carry out due diligence on vendors, especially given the rise of shadow IT and AI.

Owing to the nature of their business, fintechs are already exposed to a lot of risk. But, depending on the size of the organisation, this can be exacerbated by the number of vendors they work with. On average, fintech companies could have anywhere between 58 and 184 vendors – any number of which will be vulnerable to risk. Take for instance how vendors are leveraging AI. Unless they comply with relevant industry standards and regulations, these partners could potentially be training their models on the data fintechs provide them with – opening the door to sensitive data becoming common knowledge. This is especially damaging for fintechs because the information exchange – whether personal, financial or medical – is so high value.

But regardless, this is any issue that will leave its mark on all fintechs and unless organisations have a third-party risk management programme in place, the reputation of their business might not entirely be in their hands.

46% of organisations say that a vendor of theirs has experienced a data breach since they started working together.

How Vanta can help fintechs scale trust

Whether it's down to the size of their business or the size of their security budget, fintechs might not have the time, the tools or the personnel to manage compliance as effectively as they need to – and to keep managing it.

With Vanta, organisations can start and scale their compliance programmes so that they can get compliant faster – and stay that way – with less effort.

Benefit #1

Reducing the compliance burden

The compliance burden is at an all-time high with 11 working weeks a year spent on manual compliance tasks. There's no denying that the scale of activities required for compliance is extensive – but automation can make a huge difference.

For fintechs especially, automation is a time and money saver, and keeps teams focussed on protecting their business and innovating for the sake of their customers. On average, security teams could save between 3-5 hours a week by automating integral compliance activities such as collecting evidence for audits. For fintechs this time can be redirected to offering innovative security solutions to their customers and demonstrating why their company is the standout in its competitive marketplace.

Using Vanta, compliance teams are

129% more productive

Just ask TapTapSend – a UK-based global remittances company. With Vanta, TapTapSend eliminated the need for siloed spreadsheets and endless email threads, using automation to gather evidence for security audits and effortlessly stay on top of their security profile. They also sought PCI-DSS compliance to assure their customers that their payment information was secure and protected. This is typically a time-consuming process, but because of Vanta's continuous monitoring capabilities the work it required from TapTap Send was cut in half.

> "I saw how much time it took to gather the samples that the auditors needed last time, and that's something we want to avoid. Vanta continually monitors our PCI environment, so we won't have to scramble to find evidence at the last minute,"
>
> **Dimitrios Stergiou,** Director of IT and Information Security, TapTap Send

Benefit #2

Turning good security into good business

Measuring the ROI of trust is becoming increasingly challenging for teams. But with Vanta, teams get continuous, complete visibility across their entire programme and are able to demonstrate measurable impact and reduce risk more easily.

For fintechs, this looks like showcasing their security credentials — e.g. ISO 27001 or DORA — through a public Trust Center and using compliance to demonstrate trust to their audience. Nearly half (48%) of businesses believe good security practices drive customer trust for their business. This figure is only going up year-on-year, and for fintechs this is a direct route to beating out the competition — with trust equalling competitive advantage in sectors such as trading, lending, financial operations, and more.

This is something Silvr knows all about. With a mission to help entrepreneurs achieve success, the Silvr team offers innovative financing solutions to digital businesses, allowing them to grow without collateral requirements or equity dilution. Tasked with handling sensitive customer data, the Silvr team quickly recognised the central role of security and compliance in establishing trust with their customers. Eager to further demonstrate trust, Silvr turned to Vanta to achieve ISO 27001 certification, fuel growth in European markets and beyond, and to ensure their business wasn't disrupted in the process.

> "We really felt supported by Vanta, not just on our certification process, but also on what is the best way to approach information security."
>
> **Thomas Pelletier,** VP of Engineering, Silvr

Organisations that use Vanta see

526% ROI over three years

Benefit #3

Protecting the entire business ecosystem

Trust isn't just a reflection of your organisation – it extends to your entire network of vendors and partners. For trading fintechs, this might look like market data analysis vendors or settlement vendors; while for those operating in wealth management, this could be brokerage vendors or those in portfolio management. The point is that whatever the fintech, their operations extend far beyond their own business – and trust must extend with it.

This is why fintechs need to be able to easily discover every vendor their company works with, source vendor security information and streamline risk assessment. Vanta enables organisations to automate vendor onboarding, risk assessment, and remediation so that they can spend less time on vendor reviews and more time strengthening their security posture.

This is exactly what Ramp does. A financial operations platform, Ramp helps businesses achieve more and spend less. But this requires them to build and maintain trust at home (in the U.S) and abroad (working in 40 currencies and 195 countries). This is why PCI-DSS compliance is so vital for them – ensuring all credit card data remains secure wherever they operate, and whoever they work with.

With Vanta, teams spend

50% less time on vendor security reviews

> "Because we are in the money movement business, we operate in a highly regulated industry...What drew us to Vanta was that we wanted to partner with a solution that could help us automate a lot of our manual efforts so that we can actually scale our GRC program as our business scales."
>
> **Paul Yoo,** Head of Platform Security, Ramp

Go beyond the standard with Vanta

Fintech companies didn't start up to deal with compliance – we did.

Across Europe, countless fintechs are letting Vanta do the heavy lifting when it comes to certification so they can focus on their business and where it goes next.

Fintechs turn good security into good business

ramp
Allica Bank
Taptap Send
Qonto
SPENDESK

Discover why more than 10,000 companies choose Vanta.

VANTA.COM

Take your next step with Vanta

With Vanta, meeting and adhering to industry standards is fast, scalable and automated. Vanta helps fintechs save time on compliance, accelerate growth, securely manage vendors and demonstrate trust in protecting customer data.

This is how fintechs can focus on growing their business, innovating for the sake of their customers and demonstrating trust.

Keen to know more?
Meet with a Vanta expert today.

About Vanta

Vanta is the leading trust management platform that helps organisations of all sizes automate compliance, manage risk, and prove trust. Thousands of companies including Atlassian, Omni Hotels, Quora, and ZoomInfo rely on Vanta to build, maintain and demonstrate trust — all in a way that's continuous and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, London, New York, San Francisco and Sydney.

For more information, visit www.vanta.com.