



GUIDE (INFRASTRUCTURE PROTECTION)

Avoiding Compliance Surprises – Financial Technology



Compliance is so important in today's business economy (some might say it is the economy of business) because it is the "pass" that allows you to play. Ensure it, and you can play anywhere.

Go without it, and you're benched. From fees to jail time, PR costs to reputational damage, being caught not complying with legal standards for protecting critical systems, information, and proprietary business information has serious repercussions. In this guide, we will share ways to stay compliant with Financial Technology ([FinTech](#)) regulation requirements, the impact of compliance mistakes, and best practices for staying on the right side of the line – and in the game.

The Vital Role of FinTech

At its incipience, the term FinTech referred to the technical workings that went on behind the scenes at major financial institutions like banks. Over time, it came to be associated with customer-facing technology like digital banking, trading apps, and financial forecasting services. Today, FinTech has also expanded to encompass the use and development of cryptocurrencies like Bitcoin and Ethereum. In many ways, our vernacular understanding of financial services in 2024 is nearly entirely made up of our experience with FinTech.

Valued at [\\$294.74 billion](#) just last year, the FinTech industry is set to nearly quadruple to an amazing \$1.156 billion by 2032, displaying a robust CAGR of 16.5% within the recording period of 2024-2032.

The Vulnerability of FinTech Apps

It's an uncomfortable fact that [92%](#) of the most widely used FinTech apps contain easy-to-exploit vulnerabilities, per research by mobile app protection company Aproov. Out of a sample of 650 of the most popular financial services applications across the U.S., U.K., France, and Germany, it was revealed that:

- Over 9 in 10 (92%) leaked valuable, exploitable secrets
- 23% leaked extremely sensitive secrets
- Only 5% had adequate defenses against runtime attacks
- Only 4% were protected against Man-in-the-Middle attacks

Per the same research, an analysis of crypto apps revealed that:

- Not one out of 650 apps was completely protected
- A total of four were protected against channel Man-in-the-Middle attacks; none were in the U.S.
- 36% revealed extremely sensitive secrets (compared with 23% of general FinTech apps)

And more. The data is especially unsettling when those apps are connected to so many cards, bank accounts, and private calendars. Said Aproov CEO [Ted Miracco](#), "Have we all unknowingly become beta-testers for financial services apps?... This research shows hardcoding sensitive data in mobile apps is widespread and a massive problem since secrets can easily be extracted." And in the case of cryptocurrency, it's much worse.

What Compliance Regulations Apply to FinTech?

PCI DSS | [Payment Card Industry \(PCI\)](#) compliance, also referred to as the Payment Card Industry Data Security Standard (PCI-DSS), governs entities that store, process, and transmit credit card information from major brands. It imposes strict guidelines on the use and handling of this data, and is applicable wherever credit cards are used around the world.

Those under its jurisdiction are required to:

- Build and maintain a secure network
- Regularly test and monitor said protected network
- Implement strong access controls
- Comply with the organization's security policy
- Maintain a vulnerability management program
- And [more specifics](#)

The penalties for not complying with PCI DSS (now on [PCI DSS 4.0](#)) include:

- Payment card issuer fines
- Insurance claims
- The cost of cancelling and replacing breached cards
- License to process transactions revoked

Gramm–Leach–Bliley | The [Gramm–Leach–Bliley Act](#), referred to commonly as [GLBA](#), was a piece of legislation passed in 1999 to allow banks to offer a wider array of financial services (like investments and insurance) and govern the use of customer’s sensitive data.

It comes in three parts:

- 1. The Financial Privacy Rule** | Rules for the collection and disclosure of private information. It outlines how data is used, shared, protected, and accessed.
- 2. The Safeguards Rule** | Requires security measures to be put in place to protect private information, including administrative, physical, and technical protections.
- 3. The Pretexting Rule** | Prohibits pretexting or accessing sensitive data under pretenses, such as phishing scams and other social engineering ploys.

GLBA applicable data includes, but is not limited to, the following:

- Addresses
- Bank account and financial data
- Employment data
- Education level and academic performance
- Names
- Tax information
- Social security data
- Birth dates
- Geolocation data
- Biometric and related data
- Credit history
- Inferences drawn from other data

Finally, the overarching impact of the impact of the GLBA is three-fold:

1. Requires financial services companies to protect customers Personally Identifiable Information (PII)
2. Codifies the responsibility of financial institutions to protect personal privacy and sensitive data from unwarranted access
3. Requires cybersecurity programs within the financial sector to address data storage and security as part of written security policies

While ensuring full GLBA compliance is a many-tiered process, a few best practices include securing against [insider threats](#), keeping updated [data recovery plans](#), and ensuring all those in your supply chain are also compliant.

PSD2 | The European Union’s Second Payment Services Directive (PSD2) is a piece of legislation governing the safety of customer-initiated electronic payment transactions. This applies primarily to eCommerce activity and requires patrons to go through strong customer authentication (SCA) prior to purchasing online.

While SCA has been known to lead to higher checkout abandonment rates due to the several extra steps, the price must be paid to clamp down on a widely used attack vector – digital sales. These additional SCA steps mirror two-factor authentication (2FA) and require customers to provide:

1. Something they know (a PIN or passphrase)
2. Something they have (smartphone or smart card)
3. Something they are (biometrics and voice recognition)

The PSD2 regulations apply to countries within the EU, and Iceland, Lichtenstein, and Norway (known as the EEA), an impact:

- Payment Service Providers (PSPs)
- Financial Institutions
- eCommerce sites in the EEA
- Businesses accepting contactless offline payments in the EEA
- Companies with EEA business units

PRO TIP**Look for built-in scans, tests, and reports that can clearly relay your security posture score and network security assessment results.**

Underscoring all of these requirements is the need to show proof that you've met them, which puts the reporting capabilities of your security tools squarely in the spotlight. Not only do you need generate the type of reports that can satisfy compliance auditors, but its best if those reports are produced easily so your team doesn't burn a lot of time writing lengthy queries or reformatting.

The Impact of Compliance Mistakes

When financial institutions stay on the right side of the compliance line, there is no fanfare. On days like that, the adage "no news is good news" holds true. However, there are times when a FinTech has broken the trust between consumer and company and the price must be paid. Here are a few examples of those:

Fined by FINRA

In 2019, [FINRA](#) demanded that a well-known investing app pay out over [\\$12 million](#) dollars in restitution to the customers harmed by its failure to comply with FINRA policy. They faced penalties for violating various FINRA statutes, including "not having a reasonably designed supervisory system and procedures to achieve compliance with its best execution obligations under FINRA's rules."

In addition to the fine and consenting to a censure, the firm also agreed to take on an independent consultant to make sure their policies, systems, training manuals, and procedures were all up to date with the latest FINRA codes.

Flaw Results in a Steep Loss

A global bank and FinTech company paid a costly fee for failing to protect sensitive consumer data; however, the fine was not government-imposed. The firm lost \$20 million dollars over months due to a flaw discovered in their payment system. The error was discovered when a partner bank notified them that they had less cash holdings than expected.

The information compromised included sensitive PII such as customers names, email addresses, and partial payment card information. Combined with stolen password lists and other forms of information gleaned from the web and other heists, cybercriminals can compile detailed profiles of their victims until they have enough piecemeal data to open bank accounts, request social security card replacements, and more. While \$20 million dollars represents a hefty loss, the reputational damage of not sufficiently securing the sensitive assets entrusted to you by your customers may have more lasting, long-term effects.

Proactive Compliance Best Practices

Thankfully, some best practices can be put into place to prevent noncompliance consequences from happening. They are:

- **Catalog your infrastructure** | First, know your scope. After all, you can't protect something you don't know about. This includes knowing your vendors, as well. You need to see the entire landscape you will be responsible for securing, and if that seems intimidating, [vendor consolidation](#) is always a good way to reign those third parties in. The more best-in-breed services you can house under the same roof, the fewer architectures to have to police and patrol and the fewer compliance errors to make.
- **Utilize automation** | SOC teams are too busy to constantly make manual checks of anything and everything that could go awry. Automation is a great way to streamline processes without missing critical data. Some of the [routine business processes](#) that can be easily automated include [vulnerability management](#) and regular scanning. In this way, you can build a sustainable proactive security strategy without the constant burden of growing overhead. No matter how much your attack surface expands as your business scales, automated processes can help your security and compliance stay one step ahead of the game.
- **Put your infrastructure and employees to the test** | The end goal of compliance is ostensibly to make sure that sensitive information is safe from attackers. One of the best ways to do this is to put your defenses (and your defenders) to the test. [Penetration testing and red teaming](#) not only test the organization's ability to detect and respond to attacks but can [help FinTech organizations comply](#) with industry security standards by making sure their systems "have what it takes" to secure PII, PHI, credit card information, and other sensitive assets.
- **Test Your Applications** | Once your network and people have been put to the test, it's time to test your applications and software. Fuzz testing inputs invalid or unexpected inputs into a computer system to discover previously missed vulnerabilities or software defects. When shifted left and done earlier in the development stage, fuzzing can catch potential compliance errors before they escalate and endanger the organization. Additionally, regular fuzz testing ensures that any new additions to your security stack work as intended and deliver on the promises that your compliance policies make. This comes in handy during a security audit.
- **Get a fresh perspective** | Third-party services can help your team see what they might otherwise be just close enough to miss. An outside perspective helps when doing offensive security measures such as pentesting and red teaming because the team is unfamiliar with the security controls, the landscape, and the nuances. Coming in with a "fresh set of eyes" will simulate what an attacker sees when scoping out the network and gives the firm an idea of how an outsider might try to breach their defenses. However, there is value in developing a long-term relationship with your offensive security provider, as they will understand your vision and security needs to a greater degree than a vendor coming in entirely new. The trick? Invest in an [offensive security provider](#) that has a big enough team to put different experts on the job each time, allowing you the benefits of reduced overhead and SLAs while still giving you the "fresh eyes" that you need – with the benefit of some context around your goals, industry, and direction. This approach will enable you to more efficiently test for compliance breaches in a comprehensive way that is less prone to familiarity blind spots.
- **Keep quality compliance reports** | Lastly, it is important to maintain thorough and up-to-date records of compliance activities. There are tools that generate thorough [compliance reports](#) regularly and automatically, constantly delivering proof that an organization's systems comply with government regulations and industry requirements. Reporting is vital, but it should not be the most challenging part of compliance. Automatic and thorough reporting tools help you see where you stand in the event of an audit at all times.

PRO TIP

Compliance should be seen as the security baseline.

Compliance standards are integral but only designed as a minimum standard for adequate safety. There are many attacks that reach beyond the grasp of what can be codified and put into words – not to mention, be drafted, voted on, and approved. Consequently, there is much that can fall in between the cracks. That's why compliance should be seen as the baseline – these requirements, though a good starting point, have several limitations. They don't account for every possible threat, there are often years between updates, and they must be feasible for organizations of every size and resource level. For this reason, most organizations should be going above and beyond the minimum requirements.

Proactive Solutions and Services from Fortra

Companies in the financial services sector need best-in-breed solutions that help them not only comply with government and industry privacy and security standards but also keep them safe in a practical sense, no matter what the law. Here are some of the tools that accomplish both.

beSTORM

Fortra's dynamic application security testing (DAST) tool, [beSTORM](#), goes above and beyond. Not only does it test for millions, even billions, of potential attack combinations, but it also employs the use of a unique [black box fuzzer tool](#) that attacks an organization's defenses using the same tactics as today's advanced attackers. Additionally, it helps companies comply with the following regulations:

- ISO/SAE 21434
- PCI-DSS 4.0
- ITSAR certification
- DO-178C
- Security Effectiveness Assurance stage of AWSP

Fortra Vulnerability Management

When the [Verizon 2023 Data Breach Investigations Report](#) notes that most of the attacks it tracked in the past year were financially motivated, it's important for FinTechs to stay one step ahead of the game and keep a consistent watch on their defenses. Fortra's [Vulnerability Management](#) solution not only scans for new weak points, but continuously classifies, prioritizes, remediates, and mitigates those vulnerabilities as well. This is a key component of securing against compliance breakages within and without, accidental or intentional.

Research firm [McKinsey](#) states that FinTech revenues are set to grow three times faster than revenues in the traditional financial banking sector over the next four years. Companies in this space can expect rapid and often volatile growth; for that reason, putting a vulnerability management program on autopilot not only allows valuable resources to be allocated toward what's new and next, but allows the company to scale safely as cyberthreats continue to mount against the financial services sector.

Fortra Offensive Security

Fortra Offensive Security provides comprehensive offensive security solutions that change the game and further ensure compliance.

- [Core Impact Penetration Testing Software](#) | Powerful, do-it-yourself penetration testing software that enables even less experienced administrators to perform real-world attacks on your environment.
- [Penetration Testing Services](#) | If your SOC is strapped or needs an extra set of eyes, our Security Consulting Services (SCS) have been trusted for over 35 years to deliver expert security assessments, penetration tests, and red team engagements.
- [Cobalt Strike Red Team Tool](#) | Our high-powered threat emulation tool uses the same advanced tactics used today and comes complete with a post-exploitation agent and covert channels for adversary simulation.
- [Outflank Security Tooling \(OST\)](#) | A unique set of special red team tools developed to help you defeat encroaching attacks at every step of the kill chain. Because this toolkit emulates tactics of nation-state actors and organized crime games, some tools are released for public use – and some aren't.

Fortra Managed Services

Fortra's [Managed Security Services](#) give you the support of our experts 24/7/365. Security is hard enough. Make Fortra your relentless ally as we make your security outcomes our biggest priority. We constantly draw support and feedback from the solutions we've placed in the field and the customers who use them. We are constantly iterating and reiterating, and as our solutions continuously evolve, you can know you are getting to-the-minute protection.

Our Managed Security Services offerings include:

- Managed Detection and Response (MDR)
- Managed Data Loss Prevention (DLP)
- Managed Digital Risk Protection (DRP)
- Managed Integrity Monitoring
- Managed Web Application Firewall
- IBM i Security Services

Summary

In summary, Fortra's comprehensive [suite of proactive security solutions](#) helps FinTech organizations adhere to the compliance requirements below:

- GDPR
- PCI DSS, Gramm-Leach-Bliley Act, SOX
- HIPAA, HITECH
- FIMSA, NIST
- NERC
- CCPA, CMMC
- ISO 27001
- NIS, NDG Standards, Swift CSP

Criminal hackers will take advantage of the fact that companies often stop after meeting basic compliance safety requirements, as integral as they are. Fortra's [offensive security solutions](#) go the extra mile to ensure FinTech companies are not only compliant, but truly secure.

FORTRATM

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at [fortra.com](#).