COMPLIANCE

PROMON

DORA for financial apps: A practical approach to compliance

How application shielding can drive compliance with the EU's Digital Operations Resilience Act

Contents

4 **Introduction**

7 **Understanding the key requirements**

8 **Implementing DORA: A summary of the ESAs technical standards**

Risk assessment

Risk management

Incident reporting and management

Business continuity planning

Testing

10 **The risks faced by today's financial services applications**

Reverse engineering and tampering

Repackaging

Man-in-the-middle attacks

Data breaches

Trojans

The human risk element

13 **Enhancing DORA compliance through application shielding**

The strategic role of app shielding in DORA compliance

Runtime application self-protection (RASP): Proactive defense and swift response

Code obfuscation: Protecting the core of your mobile applications

Data encryption: Securing sensitive information at all stages

App Shielding as a pillar of regulatory compliance and security resilience

15 **How app shielding features align with specific DORA requirements**

Faster identification of suspicious activity

Reduced risk of data breaches and other attacks with code obfuscation and data encryption

Employing a multi-layered security approach to demonstrate resilience

Ensuring app functionality even during an attack for business continuity

16 **How app shielding helps in managing ICT risk from third-parties**

17 **App shielding doesn't have to negatively impact user experience**

18 **Compliance domino effect: How better app security supports compliance**

PCI DSS

PSD2

eIDAS

20 **How to implement application shielding for DORA compliance**

Managing the integration process

Managing ongoing maintenance, updates, compliance changes, and emerging threats

23 **Additional considerations for DORA compliance**

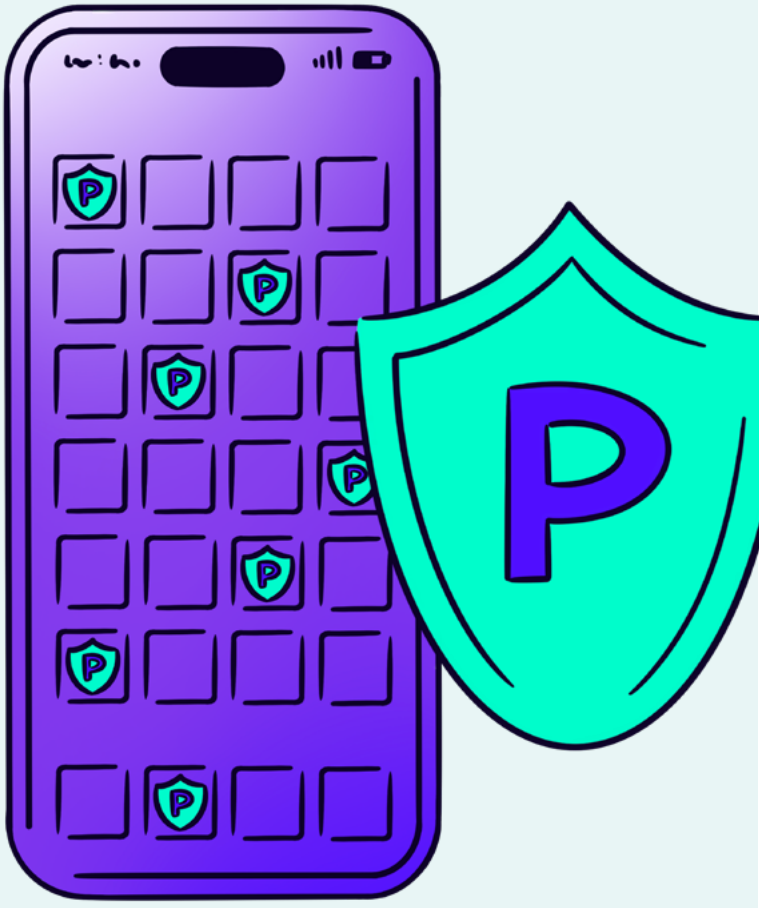
Secure coding practices

Regular penetration testing

Incident response planning

24 **Next steps for meeting DORA requirements**

25 **Promon: Your partner in DORA compliance**



Introduction

Globally, 75% of consumers use at least one app to manage their finances or make digital payments. Customers swipe, tap, and click to manage accounts, transfer funds, and invest in real time. They make payments, send invoices, and request money with ease.

But behind this seamless digital experience lies a growing concern: The mobile app security threats that put banking, payment gateway, and other financial services information at risk. As cyber threats become more sophisticated, the need for you to protect users' data has never been greater.

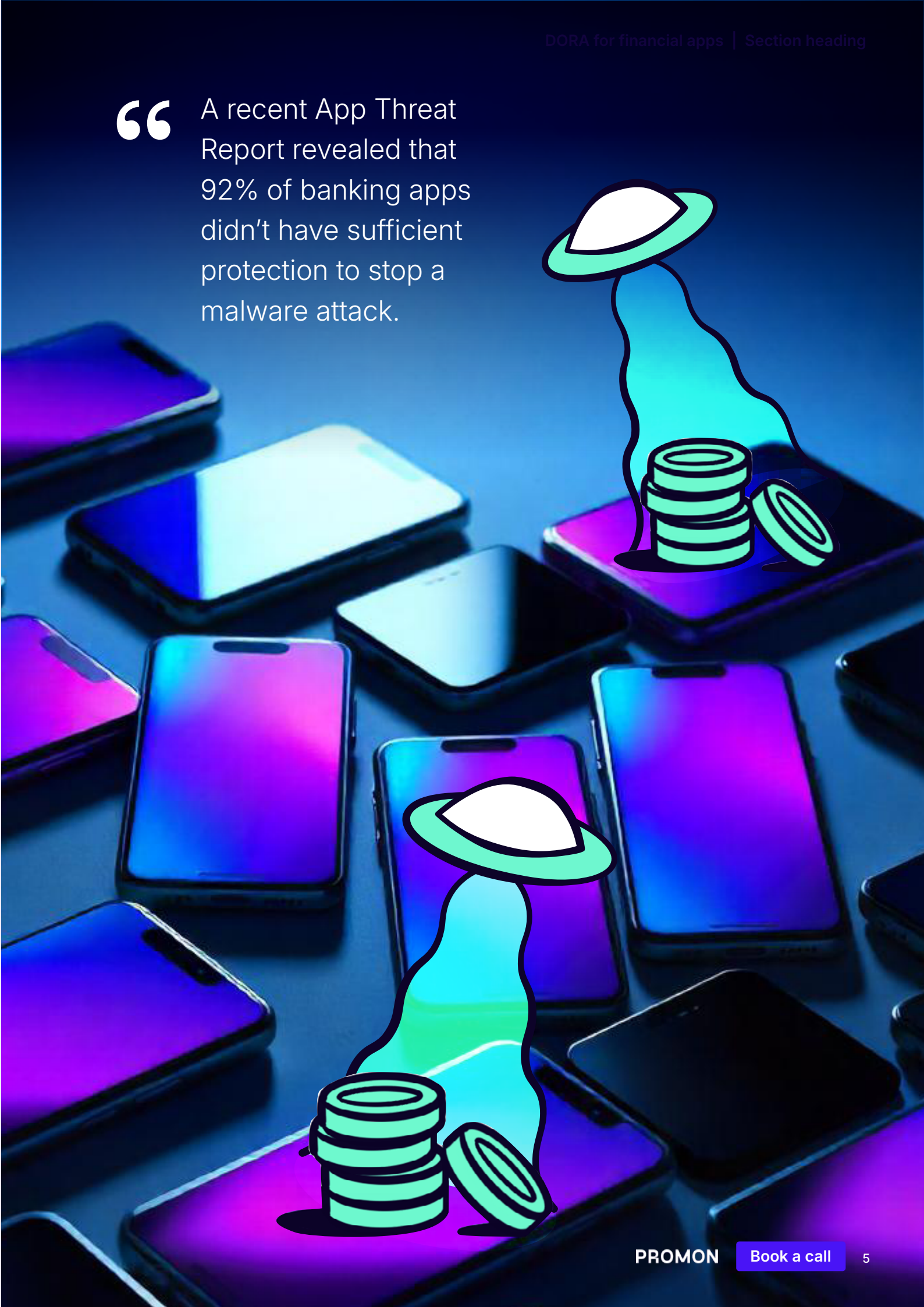
The Digital Operational Resilience Act (DORA) is the EU's regulatory response to these challenges. Over 22,000 organizations, including banks, investment firms, and insurance companies, must comply with DORA's rigorous framework for managing information and communication technology (ICT) risks.

To put the unique security challenges mobile apps present into perspective, a recent App Threat Report revealed that 92% of banking apps didn't have sufficient protection to stop a malware attack. Other research reveals that Distributed Denial of Service (DDoS) and other attacks are also on the rise.

DORA addresses these kinds of vulnerabilities by setting high standards for risk management, incident reporting, system testing, and information sharing, along with requiring practical implementation strategies that continuously improve and update to meet evolving threats. It provides a roadmap to help you better secure your digital assets, including mobile apps.

Of course, that's easier said than done. For many organizations, DORA presents an obvious (and, perhaps, overwhelming) technical challenge. In the following pages, we'll dive into the regulation and discuss how application shielding can enhance your apps' resilience—and help you achieve DORA compliance.

> A recent App Threat Report revealed that 92% of banking apps didn't have sufficient protection to stop a malware attack.



> Failure to comply comes with serious consequences.

Understanding the key requirements

DORA's designed to strengthen the EU financial sector's digital operational resilience. Its goal is to ensure financial institutions and the organizations that support them can withstand and recover from all types of ICT-related disruptions and cyber threats.

In the same way that the General Data Protection Regulation (GDPR) harmonized data privacy regulation, DORA brings standardization and best practices to managing cybersecurity challenges. It mandates that these institutions adopt comprehensive strategies and frameworks to manage ICT risks effectively, impacting a wide range of financial services entities, including:

Financial institutions:

Banks, investment firms, and insurance companies operating within the EU.

Critical third-party providers:

Entities that provide ICT services to financial institutions, such as cloud computing providers, data analytics firms, and auditing companies.

If you're among the organizations that fall under DORA, the stakes are high, as failure to comply comes with serious consequences. For example, financial repercussions are significant, with penalties as a percentage of daily turnover. In addition, non-compliance carries the possibility of audits, greater regulatory scrutiny, brand damage, and even criminal liability.

Implementing DORA: A summary of the ESAs technical standards

The European Supervisory Authorities (ESAs) develop detailed technical standards to put these ideas into practice. These standards provide specific guidelines on how you should meet DORA's requirements, and cover various aspects — such as risk management, incident reporting, testing, and information sharing — ensuring consistency and clarity in the application of the regulation. Let's take a deeper dive into some of the critical aspects of these technical standards:

Risk assessment

Under Article 15 of the regulations, DORA requires that financial institutions conduct thorough risk assessments to identify and evaluate their ICT risks. This involves areas such as identifying potential risks and understanding emerging threats and vulnerabilities. Financial services firms and your ICT partners are also required to assess the potential impact and consequence of these threats on operations and stakeholders. Finally, you must plan to regularly update risk assessments to reflect the evolving threat landscape as part of a continuous monitoring initiative.

Risk management

Effective risk management is at the heart of DORA. As part of Article 15 of the regulations, you're required to develop risk management frameworks and implement comprehensive strategies to mitigate the risks that they've identified. In addition, you're required to implement technical controls and organizational measures to prevent or respond to ICT risks. Finally, the regulations call for you to periodically review and update risk management practices to ensure the practices remain effective and relevant.

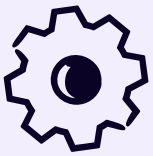
Incident reporting and management

DORA mandates that major ICT-related incidents must be reported to the relevant authorities. Under Article 16, you must have systems in place to log, track, and classify ICT incidents and if critical systems go offline this must be reported to authorities.

Per Article 19 of the regulations, you're required to report incidents that impact the ability to deliver products or services to your clients to authorities, including incidents that make clients' computers inaccessible. These notifications must be timely to support swift action and resolution. Institutions must provide detailed documentation related to incidents, including specific details, the impact, and what measures were taken to mitigate it. Finally, follow-up actions involve implementing corrective measures to prevent the issue from happening again and improve future response times.

Business continuity planning

Ensuring business continuity or the ability to stay operational in the face of specific threats is critical under DORA. You must develop business continuity plans (BCPs) for your financial organization to ensure the continuation of essential operations during and after an incident. You're also required to regularly test and update these plans to ensure they're effective and consistently being adapted to new risks and threats.



Testing

Implementing a regular testing program is another cornerstone of DORA's framework. As a financial institution, you must:

Conduct penetration testing:
Regularly test the security of systems and applications through simulated attacks.

Test incident response plans:
Ensure that incident response procedures are effective and can be executed promptly during actual incidents.

Scenario analysis:
Perform scenario-based testing to evaluate the institution's readiness to handle various types of disruptions.

Third-Party Risks

Under Article 28 of the DORA regulations, managing the risks associated with third parties is crucial. As a financial institution, you're expected to identify and manage any risk associated with your third-party ICT service providers. Potential risks include issues such as concentration risks and service disruptions. You're also responsible for ensuring your providers and vendors comply with the operational resilience standards set by DORA.

The risks faced by today's financial services applications

Implementing the recommended steps will strengthen your security posture, as well as step toward DORA compliance. But what are the threats that motivated regulators to enforce these changes?

Mobile apps in the financial sector are indispensable, yet they come with unique security risks that can have severe consequences if they're not properly mitigated. Common threats to the security of financial services apps include:

Reverse engineering and tampering

Reverse engineering involves deconstructing an app's code to understand its structure, functionality, and logic. This can lead to tampering, where attackers can modify the app's code to alter its behavior, potentially inserting malicious functions or stealing information. For example, one blockchain that supports decentralized apps relied on a specific wallet. When the wallet's code was reverse engineered, API codes were exposed and millions of dollars in cryptocurrency were stolen from user accounts.

Repackaging

In an industry where trust is everything, repackaging is a financial service provider's nightmare. Repackaging occurs when attackers modify an app and distribute it as a legitimate version. Not only does this have the potential to divert funds and endanger credentials, but it harms brands and erodes customer trust. The repackaged apps are often used for malware distribution, containing malicious code designed to seal data or cause damage. One recent example was the discovery of dozens of fake apps targeting WhatsApp users, potentially exposing private messages and accessing highly sensitive personal data including log-in credentials and even biometrics.

Man-in-the-middle attacks

Man-in-the-middle (MitM) attacks occur when an unauthorized person intercepts communications between a user and the app, potentially leading to the exposure of sensitive information, including login credentials and financial data. One of the most famous MitM attacks was revealed when Europol dismantled an organized group of 49 hackers who gained access to corporate email accounts and then monitored them for payment requests, which the hackers requested that customers divert to their accounts.

Data breaches

Data breaches often make headlines, and they're more than just reputational threats. IBM estimates the average data breach costs $4.45 million to resolve. Data breaches occur when unauthorized parties gain access to confidential data stored within the app or its backend systems. This can result in the loss of sensitive personal information, financial information, and transaction details. In 2017, for example, the US credit reporting bureau, Equifax, experienced a data breach where identifying data for hundreds of millions of people was stolen.

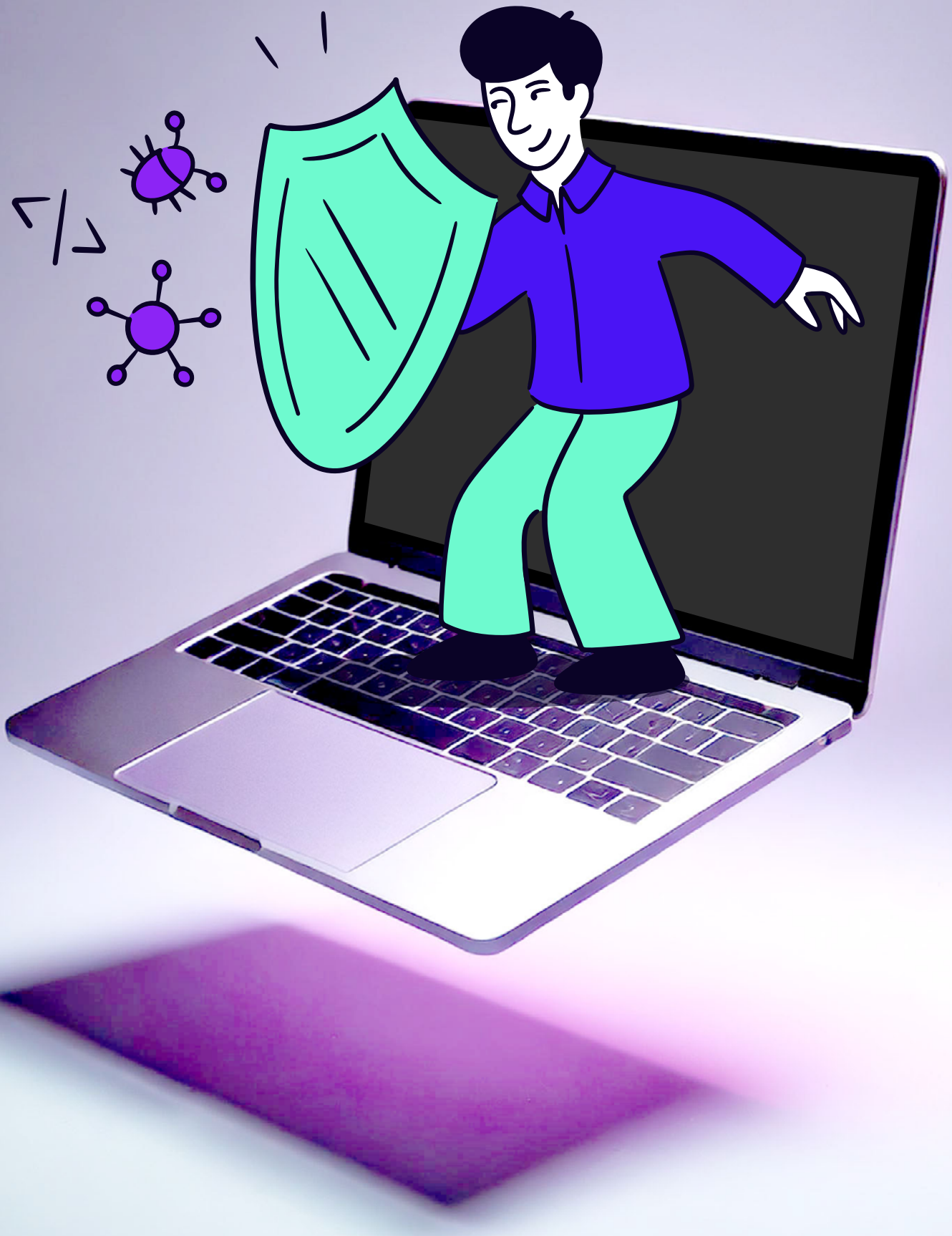
Trojans

Trojans are malicious programs disguised as legitimate software. These are often embedded in repackaged apps. When users unknowingly install them, they can steal data, collecting and transmitting sensitive user information directly to the attackers who created the program. The "Gustuff" trojan specifically targeted banking apps, tricking users into providing banking credentials and leading to significant financial and regulatory challenges.

The human risk element

End-users (and even employees) can inadvertently contribute to an app's insecurity. For example, users could run an app on a jailbroken or rooted device, leaving the app more vulnerable to threats. Downloading repackaged apps and falling for phishing schemes are other common ways that user behavior can introduce threats into the ecosystem. One Swedish bank was victim to an attack that sent phishing emails to millions of customers that installed a keylogger onto user devices and directed them to a fake site where they were prompted to enter their user credentials.

With so many potential threats, you can better protect mobile apps and, consequently, customers' data and financial assets. Employing advanced security measures, such as application shielding, regular security testing, and user education, is crucial in mitigating these threats and ensuring a secure mobile banking experience.



Enhancing DORA compliance through application shielding

Adopting robust security measures is key to protecting your financial services mobile app and helping enhance your DORA compliance. App shielding embeds protection mechanisms directly into the app, offering a proactive defense against a wide range of cyber threats.

Beyond its technical capabilities, app shielding is pivotal for achieving compliance with DORA by bolstering both the security and resilience of mobile applications—a critical component for financial services organizations as you work to deliver the best customer experience.

The strategic role of app shielding in DORA compliance

App shielding isn't merely a protective measure; it's a strategic asset in ensuring mobile applications meet the stringent security and operational resilience standards mandated by DORA. By integrating advanced technologies such as Runtime application self-protection (RASP), code obfuscation, and data encryption, you can achieve more robust security and demonstrate a commitment to regulatory compliance.

Runtime application self-protection (RASP): Proactive defense and swift response

RASP technology is a cornerstone of app shielding, offering real-time threat detection and mitigation directly within the application's runtime environment. RASP works by embedding security within the application or its runtime environment, effectively creating a self-protecting app.

It functions by intercepting all calls between the application and the system to analyze behavior and context. This includes data requests, responses, and executions. If RASP detects any anomalous or malicious behavior, such as code injection or suspicious data manipulation, it can immediately take corrective actions. These actions might include terminating a session, alerting administrators, or quarantining the app to prevent further damage.

As financial services continue to digitize, the ability to detect and neutralize threats such as code injections, unauthorized access, and other anomalies during app execution is critical. RASP doesn't just detect threats; it enables the application to autonomously respond, whether by terminating a session, blocking an attacker, or alerting your security operations team.

In the context of DORA, RASP supports incident management requirements by providing continuous monitoring and instant threat mitigation. This real-time capability ensures potential security incidents are addressed before they escalate, aligning with DORA's emphasis on operational resilience and incident response.

Code obfuscation: Protecting the core of your mobile applications

Code obfuscation goes beyond simple code scrambling; it's a sophisticated technique that transforms the application's logic into a form that's indecipherable to would-be attackers. This added layer of complexity makes reverse engineering, tampering, and discovering vulnerabilities significantly more challenging.

It prevents cybercriminals from decompiling and reverse engineering source code, and protects your apps from intellectual property theft. For JavaScript in hybrid apps and languages like Java or Kotlin in Android apps, obfuscation involves techniques like scrambling variable names and altering execution paths. Unlike encryption, which makes data unreadable without a key, obfuscation makes the code hard to decipher yet operational without decryption.

For financial institutions, where the integrity of mobile applications is paramount, code obfuscation plays a crucial role in risk management. By safeguarding the app's code, institutions can mitigate the risk of unauthorized modifications and protect sensitive operational logic, thereby ensuring compliance with DORA's rigorous risk management protocols.

Data encryption: Securing sensitive information at all stages

Data encryption is the bedrock of information security within mobile applications, particularly in the financial sector where the confidentiality and integrity of data are non-negotiable. Encrypting sensitive data, whether at rest within the application or in transit between the app and backend systems, ensures that even if intercepted, the data remains protected and unreadable to unauthorized parties.

Encryption protects sensitive data by converting it into a coded format that can only be read by someone with the proper decryption key. In the context of mobile security, encryption safeguards data both at rest (stored on the device) and in transit (sent over networks). Encrypted data cannot be deciphered without the decryption key.

By implementing robust encryption protocols, financial institutions not only protect critical information but also align with DORA's mandates on data security. This ensures that all sensitive financial data is comprehensively safeguarded, reinforcing the institution's overall cybersecurity posture.

App Shielding as a pillar of regulatory compliance and security resilience

For financial services organizations, app shielding is more than a technical solution—it's a strategic imperative. By incorporating RASP, code obfuscation, and data encryption into your mobile applications, institutions can effectively shield against a myriad of threats, ensuring real-time protection, preserving app integrity, and safeguarding sensitive data.

In doing so, you're not only enhancing your security posture but also demonstrating robust compliance with DORA's comprehensive framework. As regulatory pressures increase and the cyber threat landscape evolves, app shielding will continue to be a critical element in achieving and maintaining digital operational resilience.

How app shielding features align with specific DORA requirements

Beyond the general ways app shielding solutions help organizations achieve DORA compliance, there are specific alignments between specific DORA requirements and app shielding features. Some notable examples include:

Faster identification of suspicious activity

RASP enables real-time monitoring and detection of suspicious activity within the application. It can identify anomalies and potential threats as they occur, allowing immediate intervention.

This capability aligns with DORA's requirements for timely incident reporting and management. Faster identification of threats means financial institutions can quickly report major ICT-related incidents to authorities, comply with regulatory timelines, and mitigate the impact of these incidents more effectively.

Reduced risk of data breaches and other attacks with code obfuscation and data encryption

By making the app's code difficult to understand and tamper with, and by encrypting sensitive data, application shielding significantly reduces the risk of data breaches and other types of attacks.

These measures support DORA's emphasis on robust risk management. By proactively reducing vulnerabilities and protecting sensitive information, financial institutions can better manage ICT risks and prevent security incidents from occurring.

Employing a multi-layered security approach to demonstrate resilience

Application shielding employs multiple layers of security, including RASP, code obfuscation, and data encryption. This comprehensive approach ensures that various aspects of the app's security are covered, making it more resilient against a wide range of threats.

Implementing a multi-layered security approach demonstrates to regulators that the institution has a thorough and resilient ICT risk management strategy in place. This aligns with DORA's requirements for regular ICT risk assessments and continuous monitoring of potential threats.

Ensuring app functionality even during an attack for business continuity

By protecting the app from tampering, reverse engineering, and other malicious activities, app shielding helps maintain its functionality and integrity even in the face of an attack.

This capability supports DORA's requirements for business continuity planning and testing. Ensuring that critical applications remain operational during and after an attack is essential for maintaining business continuity and minimizing disruption. Regular testing of these security measures further ensures their effectiveness and reliability.

How app shielding helps in managing ICT risk from third-parties

Managing ICT risks from third-party providers is a significant challenge for financial institutions, especially given the interconnected nature of the industry's ecosystem.

One of the primary concerns highlighted by the Open Web Application Security Project (OWASP) in this year's Mobile Top Ten is "Inadequate Supply Chain Security". This risk emphasizes the vulnerabilities introduced when third-party components or services are not adequately secured. These vulnerabilities can lead to severe security breaches, data leaks, and operational disruptions.

OWASP notes, *"An attacker can manipulate application functionality by exploiting vulnerabilities in the mobile app supply chain. For example, an attacker can insert malicious code into the mobile app's codebase or modify the code during the build process to introduce backdoors, spyware, or other malicious code. This can allow the attacker to steal data, spy on users, or take control of the mobile device. Moreover, an attacker can exploit vulnerabilities in third-party software libraries, SDKs, vendors, or hardcoded credentials to gain access to the mobile app or the backend servers."*

The results can range from stealing information to seizing control of a user device.

App shielding is effective for helping mitigate risks from third-parties. By embedding security measures directly into the app, app shielding ensures that the app remains protected even if the third-party components or services are compromised. Key features like RASP, code obfuscation, and data encryption help maintain the app's integrity and security, reducing the overall risk from third-party dependencies.

App shielding doesn't have to negatively impact user experience

Customers want fast, frictionless experiences. While they demand security, they're not willing to embrace experience tradeoffs. App shielding is a solution that enhances security, while also keeping the end user in mind. App shielding must strike a balance between robust protection and minimal friction on the user interface/user experience (UI/UX) side.

Effective application shielding should:

- **Maintain seamless UI/UX:** Ensure that security measures do not disrupt the user experience, providing a smooth and intuitive interface.
- **Preserve functionality:** Ensure that the app's functionality remains intact and responsive, even when security features are actively mitigating threats.

When financial services organizations choose the right app shielding solution, customers won't even know that it's running in the background. From the developer side, the integration is handled quickly and efficiently without disrupting development workflows or overarching timelines.

Compliance domino effect: How better app security supports compliance

More than three-quarters of leaders worry about keeping pace with increasingly complex and sweeping regulations that impact financial services. Implementing app shielding can create a compliance domino effect, where achieving compliance with one regulation facilitates compliance with others. Even when regulations don't overlap, stepping up mobile app resilience can help meet various regulatory requirements.

Here's a closer look at how app shielding can support both DORA compliance and greater alignment with other regulations:

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure all companies that process, store, or transmit credit card information maintain a secure environment.

Connections between PCI DSS and DORA include:

- **Strong cybersecurity practices:** Both DORA and PCI DSS require organizations to implement robust cybersecurity measures to protect sensitive information.
- **Facilitated compliance:** Organizations already compliant with PCI DSS will find it easier to meet some of DORA's security requirements, as both sets of regulations emphasize similar cybersecurity practices.

PSD2

The Revised Payment Services Directive (PSD2) is a European regulation aimed at enhancing consumer protection, promoting innovation, and improving the security of online and electronic payments across the European Union.

Connections between PSD2 and DORA include:

- **Enhanced requirements:** DORA introduces stricter ICT risk management and incident reporting requirements than PSD2. In some cases, DORA replaces PSD2 reporting requirements for institutions under DORA's scope.
- **Unified security goals:** DORA and PSD2 collectively enhance the security of the EU financial sector by focusing on operational resilience and secure payment services, thus protecting consumers and financial institutions from fraud and other risks.

eIDAS

The Electronic Identification, Authentication and Trust Services (eIDAS) regulation establishes a framework for electronic identification and trust services for electronic transactions within the European Single Market, ensuring their legal validity and enhancing security and trust in digital interactions.

Connections between eIDAS and DORA include:

- **Complementary focuses:** DORA's emphasis on resilience and eIDAS's focus on trust services can work together to create a more secure environment for financial institutions operating online.
- **Integrated security framework:** Combining the resilience measures of DORA with the trust services of eIDAS ensures a robust security framework for digital financial transactions and communications.

App shielding is a critical tool for financial institutions striving to meet DORA's stringent requirements while also addressing the challenges posed by third-party ICT risks. By enhancing mobile app security through features like RASP, code obfuscation, and data encryption, institutions can protect against threats from both internal and external sources. This approach not only aids in DORA compliance but also facilitates adherence to other regulatory standards such as PCI DSS, PSD2, and eIDAS, ultimately promoting a secure and resilient financial sector.

How to implement application shielding for DORA compliance

How can organizations take concrete steps to implement app shielding as part of their plan to come into compliance with DORA? It all starts with selecting the right mobile app shielding solution.

When selecting a mobile app security solution for DORA compliance, consider the following factors:

- **Comprehensive protection:** Ensure the solution provides a range of security features, including RASP, code obfuscation, and data encryption.
- **Ease of integration:** Opt for a solution that seamlessly integrates with your existing development workflows to minimize disruption.
- **Scalability:** The solution should be scalable to accommodate the growth and evolving needs of your organization.
- **Compliance support:** Verify that the vendor offers features and support specifically designed to help meet DORA requirements, and a deeper familiarity with financial services mobile applications.
- **Vendor reputation:** Choose a vendor with a proven track record and positive reviews from other financial institutions.

Managing the integration process

Once you've selected a solution, it's important to consider how the integration process will go. Integrating application shielding with existing development workflows can be challenging, especially if the chosen solution does not offer frictionless integration.

Here's how to manage the process effectively:

1. **Initial assessment:** Conduct a thorough assessment of your current development workflows and identify potential integration points for the application shielding solution.
2. **Collaboration:** Work closely with the vendor to understand the integration requirements and tailor the solution to fit your specific needs.
3. **Phased implementation:** Consider a phased approach to integration, starting with critical applications and gradually extending to all mobile apps.
4. **Training and support:** Ensure your development team receives adequate training on the new security tools and processes. Utilize vendor support for troubleshooting and guidance.

Ultimately, ease of integration is a key selection criterion for choosing an app shielding provider. Working with a provider that has capabilities to integrate app shielding post-compilation, for example, will minimize developer friction and introduce new levels of security support without negatively impacting the end user experience.

Managing ongoing maintenance, updates, compliance changes, and emerging threats

Maintaining effective application shielding requires continuous attention to updates, compliance changes, and emerging threats. Ideally, this involves a partnership between the financial services organization and the selected provider.

Some elements to look for include:

- **Regular updates:** Keep the application shielding solution updated to address new vulnerabilities and enhance security features. Collaborate with the vendor for timely updates and choose a vendor with updates that keep pace with emerging threats.
- **Compliance monitoring:** Stay informed about changes in DORA and other relevant regulations. Adjust your security measures accordingly to maintain compliance. The right partner may be regularly providing content or updates to keep you abreast of changing information.
- **Threat intelligence:** Utilize threat intelligence services to stay ahead of emerging threats. Ensure your application shielding solution incorporates real-time threat detection and response capabilities.
- **Vendor partnership:** Treat your mobile app security vendor as an extension of your security team. Leverage their expertise and resources to personalize the solution to your needs.
- **Testing and validation:** Regularly test your mobile apps' security through penetration testing and vulnerability assessments. Validate that the application shielding measures are effective and compliant with DORA requirements.

Implementing application shielding for DORA compliance involves selecting the right security solution, managing integration with existing workflows, and maintaining ongoing vigilance against emerging threats. Working with a comprehensive, scalable, and reputable security vendor helps financial organizations effectively safeguard mobile apps and ensure compliance with DORA.

Additional considerations for DORA compliance

For financial institutions developing a DORA compliance plan, app shielding can address many of the key issues. However, complex legislation has many moving parts and you need to prepare to evaluate other areas of the organization.

The checklist below can help guide those conversations:

Secure coding practices

- **Code review:** Regularly review and audit your code to identify and fix vulnerabilities.
- **Training:** Train developers in secure coding practices to ensure they follow best practices for security from the start.
- **References:** Consult OWASP's secure coding best practices guide for a comprehensive program.

Regular penetration testing

- **Internal and external testing:** Conduct both internal and external penetration tests to identify potential security weaknesses.
- **Remediation plans:** Develop and implement remediation plans based on the findings of the penetration tests.
- **Supply chain:** Understand what testing your vendors are conducting, regularly review the results, and ensure that due diligence is being conducted for SDKs or other parts incorporated into their product code.

Incident response planning

- **Incident response team:** Establish a dedicated incident response team with clear roles and responsibilities.
- **Response protocols:** Develop and document incident response protocols, including steps for detection, containment, eradication, and recovery.
- **Drills and simulations:** Regularly conduct drills and simulations to ensure the incident response team is prepared for real-world scenarios.

Next steps for meeting DORA requirements

The deadline for DORA compliance is rapidly approaching. However, with the right plans in place, organizations will have the resources needed to achieve compliance.

App shielding is a critical component of a comprehensive DORA compliance strategy, providing robust protection against a wide range of cyber threats. Integrating advanced security features such as RASP, code obfuscation, and data encryption into their mobile apps, financial institutions can significantly improve their cybersecurity posture and meet the stringent requirements of DORA.

App shielding should be complemented with other security practices, including secure coding, regular penetration testing, and a well-defined incident response plan, to create a holistic security framework. As the threat landscape continues to evolve and regulatory requirements become more sophisticated, staying proactive and adaptable will be key to maintaining compliance.

Promon: Your partner in DORA compliance

With Promon SHIELD®, you get true multi-layered security, advanced obfuscation, and runtime protection that integrates seamlessly into your existing development workflow.

It's a post-compile solution, so you won't have to worry about changing source code or disrupting your CI/CD pipeline—deployment is fast and hassle-free. In fact, you can get going within minutes (versus days or even weeks for alternative solutions). This makes it a perfect fit for financial institutions, where security is critical, and development speed is a priority.

Banks and payment platforms choose Promon for the control and flexibility our products offer. You can choose to deploy on-premise, maintaining 100% control over your security environment. For institutions navigating complex regulatory requirements like DORA, this is significant. You're ensuring that your security measures are not only comprehensive but fully compliant. Promon SHIELD® provides layered protection that embeds deep within your app, preventing attackers from bypassing features. This helps you stay a step ahead of potential threats, safeguarding your data and maintaining your operational integrity.

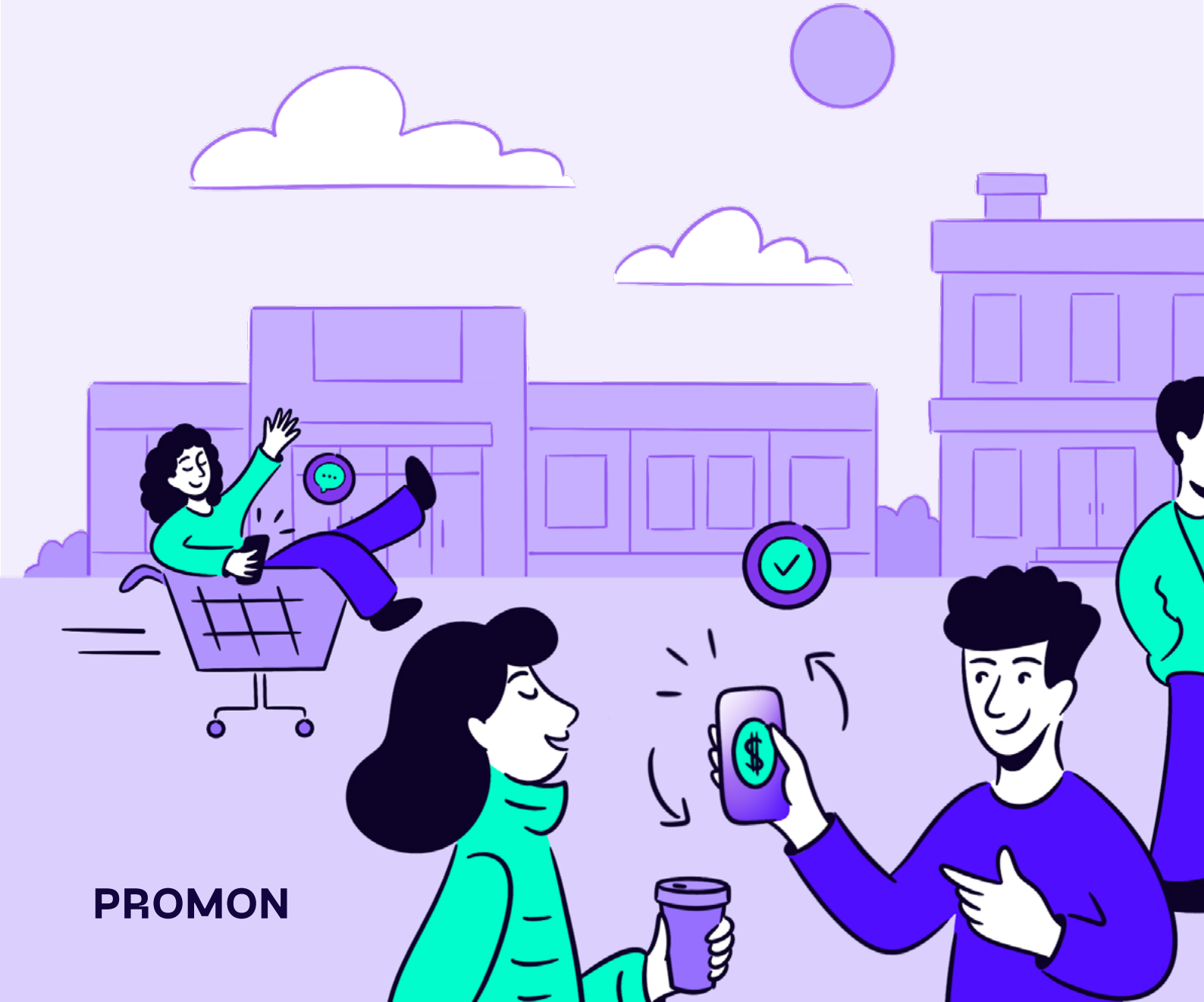
Finally, we partner with you on each step of your app shielding and mobile security journey. Our global technical support team is available around the clock to help with questions or issues, making sure you can focus on your core business without worrying about hidden fees or surprise costs. Financial institutions need stable, secure apps to maintain customer trust and meet regulatory demands, and Promon ensures that happens smoothly, boosting app performance and satisfaction at every level.

Promon is the leader in proactive mobile app security. We work to make the world a little bit safer, one app at a time.

Since 2006, some of the world's most impactful companies have trusted Promon to secure their mobile apps. Today, more than two billion people use a Promon-protected app.

Book a call

promon.co | info@promon.co



PROMON