Increasing Compliance with

Regulations in Digital Banking

A WHITE PAPER BY **JSCRAMBLER**

+1 650 999 0010 hello@jscrambler.com jscrambler.com

Table of Contents

Executive Summary

With users wanting more convenience and an easier way of handling their finances, traditional banks and fintech startups alike have started to focus on providing digital solutions for a plethora of banking services and products that were once only available through traditional brick-and-mortar banks.

However, this shift brings new risks to an already security-sensitive industry and, as such, companies should be aware of existent regulations that aim at protecting and securing the user's data. With the release of the EU's GDPR, several other countries and states have started to include consumer's right to privacy into law which has to be complied by companies operating in those locations.

Since regulations do not always give guidance on how companies should achieve the required compliance, institutions like NIST[1] and ISO[2] have released standards that provide guidance on how to improve the security posture of organizations. On a more technical side, OWASP[3] provides detailed information on the types of attacks that digital banking applications might be most vulnerable to, and solutions on how to mitigate them. Among these, we find key threats that are often unaddressed in banks, such as source code tampering and web supply chain attacks.

Jscrambler provides cutting-edge solutions to address these key threats, greatly reducing the exposure of digital banking applications to web-based attacks.

[1] https://www.nist.gov/
[2] https://www.iso.org/home.html
[3] https://owasp.org/

Introduction

Several studies have found that since the financial crisis of 2008, society's trust in traditional banks has decreased significantly. Between repaying bailouts to governments, paying fines over the abundance of regulatory failings that led to the crisis (which have totaled $321[4] billion so far), and changing their structure according to newer legislation, banks were pushed to stop their innovation front when it came to creating new products and services.

This has left an opening in the market for newer fintech companies to innovate in a stagnated industry and provide customers with new products and services that best suit their financial needs. They are developing web and mobile applications that aim at facilitating the traditional banks' over-complicated procedures and enhancing the user experience by providing user-specific advice as well as spending analytics.

Developing Banking Applications that deal with user data requires strict security practices.

4 https://economictimes.indiatimes.com/news/international/business/worlds-biggest-banks-fined-321-billion-since-2008-financial-crisis/articleshow/57438419.cms?from=mdr

In the last 10 years, the evolution of technology in the Banking industry has provided breakthroughs in multiple platforms and formats. Contactless credit cards provided a better and faster payment experience, removing the hassle of looking for change or inserting a pin code. NFC technology enabled mobile device manufacturers like Apple, Samsung, and Google to provide similar benefits using a mobile device. The improvements in the overall performance of JavaScript on the browsers and the growth of Web technologies (JavaScript frameworks and APIs, for example) shortened development cycles and enabled Banks to provide overall better experiences on the Web. Now, with the release of regulations such as PSD2, more companies are able to join the banking and fintech business and provide customer-centric solutions for money management, payments, and statistics, all within the same application.

Challenges of Digital Banking

The short answer to the question of security in Digital Banking is public concern over privacy. As each new high-profile data breach happens, the public becomes more aware and concerned about how their data is being stored and used, especially when it comes to their financial information.

When developing regular Web Applications that deal with user data, there should already be an emphasis by the development team to create a secure platform that will ensure that user data is protected.

When it comes to customers' financial information, as well as the ability to process payments for them, there should be additional focus on providing apps with

adequate security. Banks have traditionally been concerned about their security and the prevention of fraud, but the new wave of businesses that will deal with banking information do not have the same experience and expertise. As such, several regulations and standards have been put forward, so that new businesses are able to adhere to the proper security standards in banking and given a fair chance to conquer market share.

In this white paper, we will discuss the application security implications of digitalization in the banking industry. We will explore regulations and international standards that target the security of web and mobile applications in the digital banking industry and provide suggestions on how to increase compliance. Finally, we give specific recommendations for securing web and mobile digital banking applications which are aligned with the OWASP Top 10[5] and OWASP Mobile Top 10[6].

[5] https://owasp.org/www-project-top-ten/
[6] https://owasp.org/www-project-mobile-top-10/

Neobanks

When talking about traditional banks, we might think of huge organizations with widespread brick-and-mortar physical locations and a rigid structure. In opposition to that, neobanks exist only in cyberspace through the use of websites or mobile applications. Another widely used term is “challenger banks” — however, this encompasses smaller brick-and-mortar banks with a full banking license, which focus on providing better digital options for their clients, similarly to neobanks.

In the aftermath of the 2008 financial crisis, people’s trust in traditional banks dropped, as they were unsure about the safety of their money within these institutions. Also, the existence of hidden fees and over-complicated procedures just helped the growth of discontent over banks by the younger generations. Both of these reasons built up the need for neobanks.

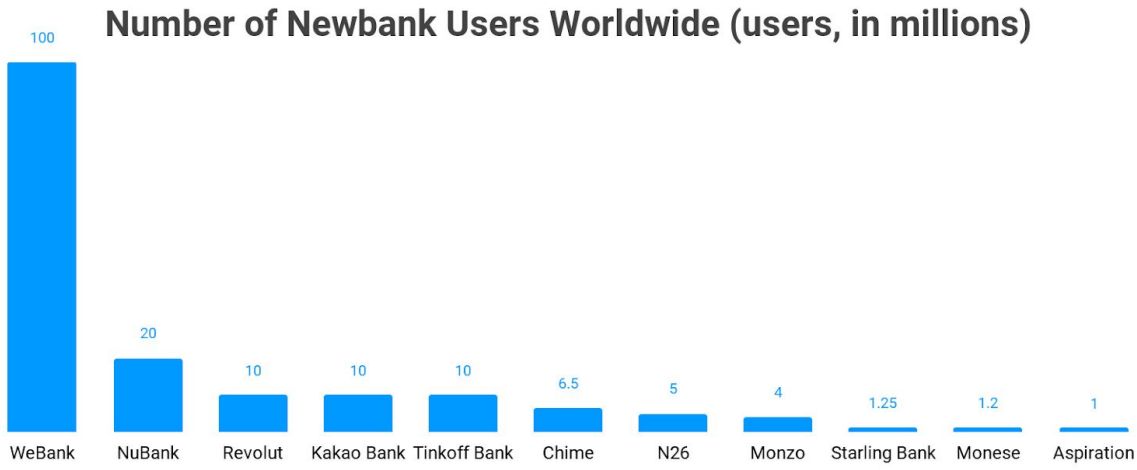

Fig. 1 — Number of client accounts of some Neobanks as of Q1 2020.

Neobanks defy incumbents by removing the existent barriers in the banking procedures in a transparent and easy to use way. They target mostly tech-savvy people and unbanked people in developing countries, where access to traditional banks is not possible for parts of the population. This is the case of Latin American countries like Brazil and Mexico, or southeast Asian countries like Singapore that have seen a significant increase in this market over the last few years.

While “neobanking” encompasses a wide range of new companies, the products each neobank can offer differ depending on what kind of licensing they have. Unlike traditional banks, that have full banking licenses and as such have to follow regulations for all the services they provide, neobanks can choose to specialize in one particular service and obtain a specific license for that. Some neobanks have applied and successfully obtained a full banking license and, as such, are allowed to offer the same type of services a traditional bank would, while remaining fully digital. Others choose to partner with a traditional bank and create an interface for the products they have, while adding advanced features for payments, money management, and spending analytics.

As more and more Neobanks enter the market and Digital Banking services grow, **it's crucial to ensure that these platforms are able to keep customer data secure**. While most neobanks and fintech businesses are not full-fledged banks (and thus not required to follow all the regulations traditional banks have), they still have to follow regulations when it comes to consumer privacy.

Regulations

Regulations directly answer the need for improved security when it comes to protecting customer data in digital banking. The need to comply with these regulations is mostly tied-in with the type of services provided by the bank and its operating country.

Here, we will approach three regulations directly related to the financial industry — PSD/2, 23 NYCRR 500, GLBA, and *Sistema Financeiro Aberto* — as well as three regulations that are aimed at consumer privacy in general (which the financial industry is also subject to) — GDPR, CCPA, and LGPD.

For each regulation, we will present the general goals that lead to the creation of the regulation, and then provide a summary of how organizations can increase compliance. In the final section, we put forward practical recommendations to increase compliance by putting in place application security best practices.

PSD2

The Payment Services Directive 2 (PSD2) was adopted by the European Commission in 2015, replacing the original Payment Services Directive of 2007. Like its predecessor, PSD2 affects the regulation of payment services in the EU and EEA. It was created with the intent of increasing competition in the financial industry by allowing non-banks to participate and harmonize compliance standards for payment providers. It also focuses on enhancing protections for online consumers

and their rights by introducing a greater degree of transparency in payments, and new rules for surcharges, currency conversion, and the way complaints are handled.

Another significant legislative effect is that PSD2 enables third-party access to account information held by banks. With customer authorization, these third-party companies may now retrieve account data from banks directly when they need to process a payment, without having to go through an intermediary service provider. This new access is managed by open APIs (developed and released by the banks themselves) which effectively enable third-parties to build a new market of financial services and products on top of the existing infrastructure that banks have in place.

PSD2 also regulates two types of third-party services that were already in existence, but without a clear regulation: Payment Initiation Services (PIS); and Account Information Services (AIS). **AIS providers** aggregate a customer's banking information from one or multiple banks and accounts, allowing a global view over their financial situation and an easier way of analyzing their spending habits. **PIS providers** facilitate the use of online banking to make online payments. These services help to initiate a payment from the consumer's account to the merchant's account by creating an interface to bridge both accounts, filling in the information needed for the bank transfer (amount of the transaction, account number, message) and informing the store of the transaction. PSD2 also allows clients to make payments to a third-party from a bank's app using any of the client's accounts (whether they belong to this entity or not).

Achieving PSD2 Compliance

One important security feature introduced by PSD2 is the Strong Customer Authentication (SCA) criteria that banks are required to use. This can be accomplished by two-factor authentication based on the following concepts:

- **Something you know**: Provide unique information only that customer will know. E.g., password, response to a security question, or PIN;
- **Something you have**: Have access to a device that is only associated with the customer. E.g., Two-factor identification via mobile phone;
- **Something you are**: Show physical proof. E.g., biometrics, such as fingerprint or facial recognition.

Third-party service providers have to require a license for the type of business they provide from the European Banking Authority (EBA). Also, Payment Service Providers (which includes both banks and third-party providers) are required to have valid digital certificates that comply with the Electronic Identification, Authentication and Trust Services (eIDAS) regulation to guarantee the required levels of authentication, confidentiality and integrity for payment transactions.

In the case of remote payments or fund transfers, an authentication code must be generated and "dynamically linked" to the transaction, meaning it needs to take into account the transaction's amount and beneficiary. This allows for traceability over the transaction and the detection of any tampering attempt to the transaction details.

23 NYCRR 500

New York City is one of the biggest financial centers of the world and home to some of the largest stock exchanges. As such, it was important to guarantee that financial institutions working in the state of New York followed tighter cybersecurity regulations in order to protect such a core service for the country.

In 2017, the New York State Department of Financial Services (NYDFS) introduced new cybersecurity regulations for financial services companies to address the growing threats posed by criminals on financial institutions. These regulations include 23 sections outlining requirements for developing and implementing an effective cybersecurity program. They require financial institutions to assess their cybersecurity risks and develop a plan to proactively address them to ensure the protection of customer data and security of operations within the industry.

Achieving 23 NYCRR 500 Compliance

Most of the 23 sections in this cybersecurity regulation share the same objectives as industry standards like the ISO/IEC 27001:2013 (which we will mention later in the document). These objectives are related to performing a risk assessment of the institution, defining security policies to mitigate damages against the identified threats and a plan for implementing such policies into the company. However, the regulation also mentions additional requirements that companies have to follow in order to be compliant with the regulations and be allowed to operate in the state of New York:

- Designation of a Chief Information Security Officer (CISO) to oversee and enforce the security policies (some small companies may be exempt from this requirement);
- Anual Penetration testing and bi-annual vulnerability assessments over the institution's information systems;
- Use of multifactor authentication to protect against unauthorized access to Nonpublic Information or Information Systems;
- Notify the State's Superintendent when a security incident affects the institution operations, as well as a yearly report covering the previous year.

GLBA

The Gramm-Leach-Bliley Act (or GLBA), also known as the Financial Modernization Act of 1999, is a United States federal law. It has two main objectives that target all financial institutions operating in the U.S. The first was to repeal the Glass–Steagall Act and the Bank Holding Company Act of 1956, allowing commercial banks, investment banks, securities firms, and insurance companies to consolidate and provide all these services to their customers. The other goal was to expand and tighten consumer data privacy safeguards and restrictions and make it mandatory for financial institutions to explain how they share and protect their customers' private information. For IT professionals and financial institutions, it is then necessary to secure and ensure the confidentiality of customers' private and financial information.

Financial institutions must also communicate to their customers how they share their customers' data, informing them of their right to opt-out of sharing the data with third-parties.

The primary data protection implications of the GLBA are outlined in its Safeguards Rule, describing what steps the institutions should follow to properly protect and manage customers' private data. The GLBA is enforced by the FTC, the federal banking agencies, and other federal regulatory authorities, as well as state insurance oversight agencies.

Achieving GLBA Compliance

GLBA requires that financial institutions act to ensure the confidentiality and security of customers' "nonpublic personal information," or NPI. The Safeguards Rule states that financial institutions must create a written information security plan describing the program to protect their customers' information. The information security plan must be tailored specifically to the institution's size, operations, and complexity, as well as the sensitivity of the customers' information. According to the Safeguards Rule, covered financial institutions must:

- Designate one or more employees to design and implement an information security program;
- Make a thorough risk assessment to customer information in each relevant area of the company's operation and evaluate the effectiveness of the existing measures in mitigating the risks;
- Design and implement a safeguards program and regularly monitor and test it;
- Use third-party service providers that are also certified and able to provide the same level of protection to customers' data;
- Continuous updating of security measures implemented in the institution;
- Provide efficient employee management and training;

- Constant monitor of security measures that are safeguarding user's data;

Open Banking Brazil

In May of 2020, Brazil's Central Bank approved the guidelines for banks and fintechs to follow in order to implement the *Sistema Financeiro Aberto* (Open Banking) in the country. Following the EU's PSD/2 legislation, this system aims at improving the efficiency and increasing the competitiveness in the country's financial market.

As consumers are the owners of their own financial data, this legislation will allow them to use different applications to manage their finances. With banks and fintech companies being required to provide open APIs, it paves the way for new applications to be created that better fulfill consumers' needs.

In terms of the security concerns known so far, applications can only access financial content from banking institutions with the user's explicit consent. Financial data is also covered by the *Lei Geral de Proteção de Dados* legislation that we will approach later on in this paper that is to be finalized in the summer of 2020. This means that secure measures need to be applied to all the information used in this new financial system - which also means that new and existing applications must have an authentication system at least as strong as the ones currently used by banking institutions.

GDPR

The European Parliament adopted the General Data Protection Regulation (GDPR) in April 2016, replacing an outdated data protection directive from 1995. It carries provisions that require businesses to protect the personal data and privacy of EU

citizens for transactions that occur within EU member states. The GDPR also regulates the exportation of personal data outside the EU.

What this means is that all existing contracts with data processors (e.g., cloud providers, SaaS vendors, or payroll service providers) and customers need to spell out responsibilities. The revised contracts also need to define consistent processes for how data is managed and protected, and how breaches are reported.

The GDPR places equal liability on data controllers (the organization that owns the data) and data processors (outside organizations that help manage that data). A third-party processor not in compliance means your organization is not in compliance. The new regulation also has strict rules for reporting breaches that everyone in the chain must be able to comply with.

The GDPR gives 4 basic rights to data subjects:

1. Transparency and modalities from data controllers, by providing consumers information on how their data is being used in a concise, transparent, intelligible, and accessible way, using clear and plain language, in particular for any information addressed specifically to a minor;
2. Data controllers have to give data subjects access to their personal data and information about how this personal data is being processed. A data controller must provide, upon request, an overview of the categories of data that are being processed as well as a copy of the actual data. Furthermore, the data controller has to inform the data subject on details about the processing, such as the purposes of the processing, with whom the data is

shared, and how it acquired the data. A data subject must be able to transfer personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller

3. Data subjects have the right to request the rectification and erasure of personal data related to them on any one of a number of grounds within 30 days, including noncompliance
4. The GDPR allows an individual to object to processing personal information for marketing, sales, or non-service related purposes. This means the data controller must allow an individual the right to stop or prevent controllers from processing their personal data.

Achieving GDPR Compliance

To be compliant with GDPR, data controllers and data processors have to follow different regulations and guidelines when dealing with consumers' data. The first move towards achieving that goal is to perform an assessment over the data that is gathered and processed by the company. It is important to know where it comes from, what it is, the reason behind its collection, how it is handled and removed.
Another important step is to provide employees the correct training over the importance of data protection. This will then impact existing operational policies, procedures, and processes to be compliant with the data protection goals of the company, or even the creation of new ones in areas where they did not exist before.

On a more technical side, companies are required to update their usage policies on websites, as well as inform and request consent from users before being able to gather information on them, traditionally done with the use of cookies. Existing

forms that ask for user information must now explicitly state what the information will be used for. If there is more than one use case for the user information that must also be explicit in different opt-in options.

Data at rest or in transmission must also be pseudo-anonymized to ensure its security against a malicious agent, and this can be achieved in two ways. The first one is through the use of cryptography, eg. TLS for network traffic and AES for storage. The other one is through a tokenization process, where sensitive data is replaced for a generalistic token, for example, converting *user@company.com* to [*email]*. This is a faster and lighter approach when the specific data contents are not necessary for the company business, which is the case of analytics solutions.

CCPA

The California Consumer Privacy Act (CCPA), is a state law introduced in 2018 that became effective at the beginning of 2020. This law enhances consumers' privacy rights and protections for residents of the state of California in the United States. More specifically, it gives customers the right to demand companies to share the information they have collected from them as well as possible third-parties that have had access to such data as well. It also gives the right to opt-out of the sale of their information to other companies as well as to request the deletion of any personal information that the company has collected from the consumer.

There are two main differences between the CCPA and the GDPR. Firstly, CCPA has a broader approach to what constitutes sensitive data when it relates to a particular user. Secondly, whilst the GDPR makes it mandatory for companies to ask for consent from the user before collecting information from them, the CCPA only

makes it a requirement for children under the age of 13 to have a parent or guardian giving consent, and for teenagers between the ages of 13 and 16 to give consent for data to be collected from them.

Achieving CCPA Compliance

Since this law does not specify how data should be collected, stored or managed, the main requirements for a company to be compliant with the law are as follows:

- Implement consent forms for minors under 13 years aimed at parents or guardians and the affirmative consent of minors between 13 and 16 years for data sharing purposes;
- Add a “Do Not Sell My Personal Information” option on the website of the business, that will direct users to a web page enabling them, or someone they authorize, to opt-out of the sale of the resident's personal information;
- Designate methods for submitting data access and deletion requests, including, at a minimum, a toll-free telephone number;
- Update privacy policies with newly required information, including a description of California residents' rights.

LGPD

“Lei Geral de Proteção de Dados Pessoais” is a Brazilian law similar to the EU's GDPR that will come into effect in August of 2020. The law aims at protecting consumers’ right to privacy when it relates to their data. It regulates how users should be asked for consent before sharing any information with the company and for what specific purpose it will be used for. Consent can not be given by minors and should instead be given by parents or guardians.

At any point in time, consumers should be allowed to review what information a company has on them, request to change it, for anonymization or even deletion from the company databases. Users can also request to know what their information was used for at any point in time, if it was shared with third parties, and can even revoke their consent at any point.

In the case of a security incident that might compromise the security of the customer's data, this has to be communicated to the proper authorities and the affected consumers.

The requirements for compliance are mostly similar to the ones for GDPR, except when it comes to the position of a Data Protection Officer, which in GDPR is only required in some cases, while in LGPD it appears to be mandatory for all companies, according to article 41.

International Standards

Some of the regulations mentioned here share the same goals as existing Cybersecurity standards created by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). Namely, the NIST cybersecurity framework and the ISO/IEC 27000:2018 provide the necessary guidelines for companies to be compliant in terms of security. At the same time, new standards are being created with a common set of guidelines to help in the development of banking and financial applications with the goal of facilitating the adoption of the existing and future regulations.

Open Banking

Whilst PSD2 defines that banks should have secure APIs to be accessed by third-party providers, it does not define a standard way on how that can be achieved. As such, the UK government (more precisely, the Competition and Markets Authority (CMA)) created Open Banking Limited, a non-profit company, which puts forward the standards on how those APIs should be created and used.

APIs should have bank-level security, with rigorously tested software and security systems so that only your bank will have access to your login credentials. They should also be regulated by the proper authorities so only approved apps and websites are allowed to access your bank with your permission.

NIST Cybersecurity Framework

The NIST cybersecurity framework is an agglomeration of existing standards and guidelines to help organizations manage and reduce their overall cybersecurity risk.

Fig. 2 — Nist's Cybersecurity Framework[7]

[7] https://www.nist.gov/cyberframework

The core of the framework can be divided into 5 functions that present the key cybersecurity outcomes expected from the company. These functions are Identify, Protect, Detect, Respond and Recover.

- The Identify Function assists in understanding the business context, the resources that support critical functions, and the related cybersecurity risks in a company. It then enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- The Protect Function outlines appropriate safeguards to ensure the delivery of critical infrastructure services. These include defining access control policies, providing awareness training sessions to employees, protecting data storage and continuous maintenance of the infrastructure.
- The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. It includes the continuous logging of security-related occurrences, monitoring of such events and the quick identification of any anomalous events.
- The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. It should include response planning for possible incidents, communication guidelines as well as mitigation actions that should be put in place.
- The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. Alongside the recovery planning, measures should be improved, if necessary, across the other functions in this framework.

ISO/IEC 27001:2013

The purpose of ISO IEC 27001 is to help organizations establish and maintain an information security management system (ISMS). An ISMS is a set of interrelated elements that organizations use to manage and control information security risks and to protect and preserve the confidentiality, integrity, and availability of information. To successfully be compliant with the norm, the standard defines 7 important points that need to be followed:

1. **Organization context:** Before going into security technical implementations, it is first necessary to understand the organization's context, what information it is trying to protect and who are the owners of such information.
2. **Leadership:** The management team needs to establish and ensure that information security objectives and policies are being properly implemented and are compatible with the strategic goals of the company. It also needs to ensure that the required resources are allocated to the information security management system.
3. **Planning:** Based on the issues defined on the first point, the company should do a risk assessment over the information that shall be covered by the ISMS, define risk acceptance criteria and construct a plan on how to prevent or reduce the effects of security incidents as well as improvements to the ISMS.
4. **Support:** The company has to ensure they have the correct resources and competences to maintain the ISMS, provide security awareness sessions for their workers, and properly document procedures and policies related to ISMS so that they are readily available.
5. **Operation:** Companies must plan, implement and control the security processes defined before to fulfill the requirements set for the ISMS.

6. **Performance evaluation:** Companies need to define what processes and controls need to be monitored and measured, continuously monitor those assets and analyze their performance to ensure valid results from the system. Companies are also advised to conduct audits in different areas of the ISMS at different points in time to validate their correct implementation.
7. **Improvement:** As the company evolves, as well as technologies, companies need to have a nonconformity attitude towards their ISMS and have continuous improvements over the system to guarantee its suitability, adequacy and effectiveness over time.

ISO 12812:2017

With customers relying more and more on their mobile devices to take care of their financial tasks, it is paramount for businesses to have a standard they can follow to best protect their users. ISO 12812 is a set of definitions commonly agreed by the international financial industry that help define a general framework of how mobile financial services (payment and banking services involving a mobile device) should be constructed. The standard is split into 5 parts, each one tackling a different aspect of the framework:

- ISO 12812-1 General Framework and Common Terminology – This defines the general framework of mobile financial services (MFS — payment and banking services involving a mobile device). It facilitates interoperability between different mobile payment systems.
- ISO 12812-2 Security and Data Protection – A Security Framework including an analysis of vulnerabilities, threats, and countermeasures for the operation of MFS. It also includes security measures to handle data at rest and in transit as well as information on key management systems associated with the data.

- ISO 12812-3 Application Management – This document specifies the interoperable lifecycle management of applications used in mobile financial services. It deals with different types of applications (covering authentication, banking, and payment applications) as well as credentials. The document also includes guidelines for several types of application architectures.
- ISO 12812-4 Mobile Payments to Persons (P2P) – This document provides comprehensive requirements and practices involved in mobilizing the transfer of funds as well as specific use cases for the implementation of interoperable mobile payments to persons. It includes guidelines for payments where payer and payee are physically close to each other and technology like NFC can be used to process payments, and also for payments where payer and payee are not physically present for the interaction.
- ISO 12812-5 Mobile Payments to Business – It focuses on mechanisms by which a person (“consumer”, “payer” or “business”) uses a mobile device to initiate a payment to a business entity (“merchant” or “payee”). Such a payment may use the traditional merchant point of interaction (POI) system, where the manner of settling the payment follows well-established merchant services paradigms.

Practical Recommendations

In addition to the regulations and standards described earlier, in this chapter we provide actionable recommendations that can be applied to both web and mobile applications with the goal of improving their security and reducing the attack surface. We are dividing these recommendations into three fundamental areas: **Server-side**, **Network**, and **Client-side**.

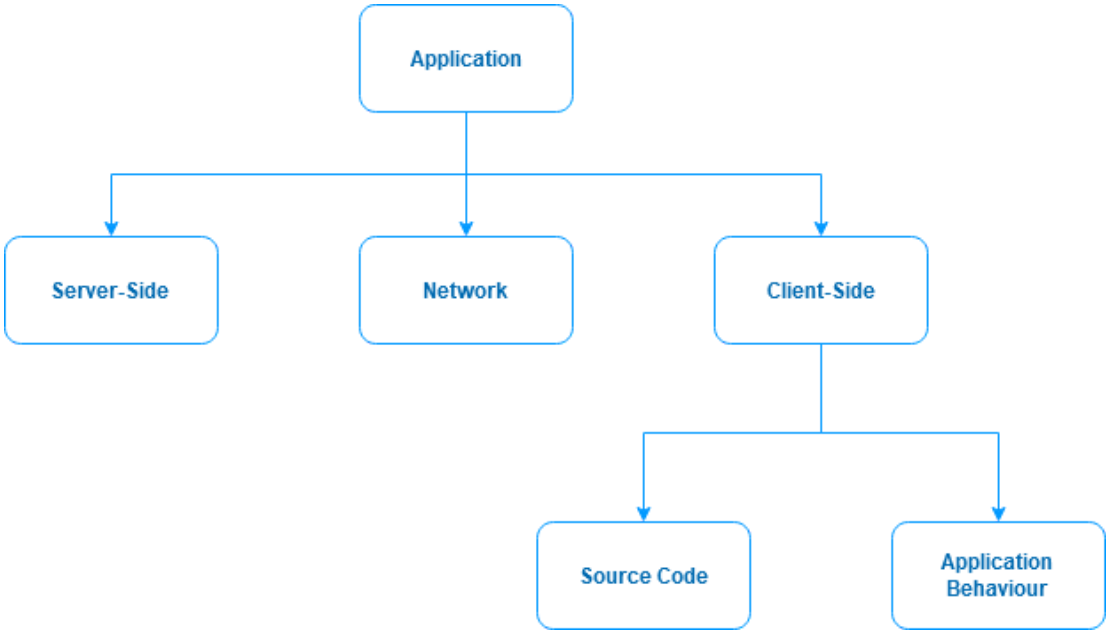

Fig. 3 — Application Security Areas

These recommendations are aligned with the ones provided by OWASP. While the regulations and standards explored before might not directly pinpoint these security practices, following them will help reduce the number of attack vectors a malicious agent might use to exploit the web/mobile application, exfiltrate consumer data, and thus cause the company to be non-compliant with regulations.

Server-Side Security Recommendations

1. **Input Validation:** Sanitization of all inputs coming from the user/outside should be considered malicious and as such should be properly validated to deter any malicious action to propagate to the server and/or other users.
2. **Restrict Access Control:** Non-public rest services must perform access control at each API endpoint either through authentication or security tokens. The enforcement of roles and permissions for each user should be done server-side and not on the device running the application (both web or mobile). In the case of mobile applications, the storage of any kind of authentication info in the device should be avoided, as this can easily be leaked by an attacker.
3. **Validate Content Types:** The body of a request/response should match the intended content type in the header. Otherwise, this can cause misinterpretation at the consumer/producer side leading to code injection or execution.
4. **Error Handling:** Keep error messages as generic as possible. This will reduce the amount of information a potential attacker can gain when they are trying to game the system or perform a secondary attack with the new information.
5. **Audit Logs:** It is important to store logs of web activity generated by the application or a malicious actor trying to attack either the server or the application. This information will then allow the organization to more easily investigate security incidents, discover their origin and make improvements to mitigate future attempts.

6. **Cross Origin Resource Sharing (CORS):** In the case of web applications, you should have a well defined CORS policy, so the browser is aware of which cross-domain requests are permitted by the application. This way, only the specified domains are allowed to make JavaScript calls to the REST service.
7. **Security testing:** During development, debugging code is added to the server-side to verify the behavior of each endpoint. However, before deploying the application to production, it is necessary to remove all the extra code that is unused, since an attacker can use that extra information to exploit the application.

Network Security Recommendations

1. **Use HTTPS:** An SSL/TLS connection protects authentication credentials in transit such as passwords, API keys, or JSON Web Tokens. It also allows clients to authenticate the service and guarantees the integrity of the transmitted data. Also, it is advised to use TLS 1.2+ as previous versions have been deprecated due to their vulnerabilities.
2. **Manage Endpoints:** There are a couple of things you can do to securely manage your endpoints. Avoid exposing your management endpoints by way of the Internet. If your management endpoints must be accessible to the Internet, make sure that all users authenticate using strong authentication mechanisms such as multi-factor authentication. Exposing management endpoints by way of different HTTP ports or host them on different/restricted subnets can also reduce some risk — however, these should be seen as additional measures and not standalone. Lastly, restrict access to these endpoints by firewall ACLs.

3. **Security testing:** Before deploying the application to production, it is important to verify that only the required endpoints are available to the outside. All other services should be protected inside the server network and behind a Firewall.

Client-Side Security Recommendations

Source Code Protection Recommendations

1. **Know your target platform:** When designing a new application, you should be aware of (and implement) platform-specific best security practices. Web, Android and iOS all have different specifications when it relates to security. As so, an app that's secure in one platform may not be secure in another one.
2. **Code Cleanup:** During development, it is often the case to add debugging code, as well as comments, throughout the application to facilitate several tasks, including testing. However, before deploying the application to production, it is necessary to remove all the extra code that is unused, since an attacker can use that information to create a successful attack on the application or the server behind it.
3. **Detection and Prevention of Code Tampering:** A property of both web and mobile applications is that it is delivered and run on the client-side. As a result, this code is vulnerable to tampering by possible attackers. To counter this, the application must be able to detect at runtime when its code has been tampered with (through additions or changes) and react accordingly to stop the attack.

4. **Detection and Prevention of Reverse Engineering:** It is not uncommon for attackers or competitors to try and reverse engineer the logic of applications to replicate these features for self-gain. A known suitable approach to prevent this is using code obfuscation to greatly increase the difficulty of determining logical connections between parts of the code.

Jscrambler JavaScript Protection

Jscrambler is specialized in protecting the JavaScript source code of web and mobile applications against **code tampering** and **reverse engineering**, two topics presented before (and highlighted by OWASP) and which typically are not covered by banking institutions.

Jscrambler Code Integrity achieves first-class JavaScript protection by adding up to 3 security layers: **Polymorphic Obfuscation**, **Code Locks**, and **Self-Defending**. As a result, the protected code will be resilient to all reverse engineering tools and techniques, while also preventing any type of code tampering or debugging. When attackers attempt to tamper with code protected by Jscrambler, it will automatically break to stop the attack and the Jscrambler real-time Dashboard displays details about the attack and the attacker.

By integrating Jscrambler into their build process, banking institutions can ensure that every code build is protected.

Application Behavior Recommendations

1. **Input Validation:** Client-Side sanitization can help the user-experience by minimizing the server-side round-trips to validate input correctness (eg.

correct email input construction), but ultimately all security validation should be done server-side.

2. **Cleanse Sensitive Information in HTTP Requests:** When sending sensitive information through an HTTP request, avoid using this information in the construction of an URL. Instead, use it as part of either the Header or the Body of the request, depending on the type of request. This is important as URLs are captured by web server logs which might create an unnecessary security breach.
3. **Error Handling:** Keep error messages as generic as possible. This will reduce the amount of information a potential attacker can gain when they are trying to game the system or perform a secondary attack with the new information.
4. **Audit Logs:** It is important to store logs of web activity generated by the application or a malicious actor trying to attack either the server or the application. This information will then allow the organization to more easily investigate security incidents, discover their origin and make improvements to mitigate future attempts.
5. **Local storage:** If your application requires storing sensitive information locally, use standard and secure algorithms to encrypt and protect the data in the local device.
6. **Prevent Web Supply Chain Attacks:** Development teams are often required to meet strict deadlines for quick product releases. As a result, developers rely extensively on third-party libraries and dependencies to fulfill some of the application's requirements. However, third-party libraries (or their own dependencies), can become compromised and then silently ship malicious code into your own application. As such, it is important to regularly vet

externally sourced code, as well as be able to detect malicious behavior on the application regardless of the attack vector.

Jscrambler Webpage Monitoring

Jscrambler Webpage Integrity (WPI) is a holistic solution to detect and prevent malicious code from tampering with the client-side of web applications and leaking sensitive data — such is the case of **web supply chain attacks** as presented above.

With the average web/mobile application containing thousands of pieces of externally sourced code, vetting this code systematically is often not possible. Also, attackers have been evolving the malicious code used in web supply chain attacks to bypass several detection techniques. The attack surface is so extensive that there is often no guaranteed way of preventing this type of malicious code injection.

Unlike other solutions that are often bypassable or introduce significant overhead, Jscrambler WPI is a behavior-based solution, resilient to any form of bypass, that provides real-time visibility of any type of web supply chain attack. With WPI in place, banking institutions can quickly detect and block data exfiltration attempts and greatly reduce their attack surface.

In-Depth Security

After navigating the most relevant regulations, standards and security best practices for banking organizations, it becomes clear that the path to compliance is paved by a deep understanding of the attack surface and employing the right security

solutions. This means extending security from the server-side to the network and the client-side.

In order to minimize exposure to data exfiltration and maximize compliance with regulations, **organizations must pay special attention to lesser-known gaps in client-side security**, such as the exposed source code of their applications and the growing threat of web supply chain attacks.

Jscrambler's technology addresses these key client-side security threats in digital banking. This solution is trusted by some of the top 20 global banks and is recognized by Gartner in the market guides for In-App Protection and Online Fraud Detection.

Contact Us

If you want to know more about how Jscrambler can help you secure your banking application, don't hesitate to contact us

hello@jscrambler.com

+1 **650 999 0010**

Gartner®

Jscrambler is the leader in Client-Side Application Security Recognized in **Gartner's Market Guide for Online Fraud Detection** and in **Gartner's Market Guide for In-App Protection**