Bambora Security and Privacy Information FAQs

Who is Bambora?

Founded in 2015, Bambora is a collection of companies with decades of experience in the payments industry. With offices around the world, Bambora provides payment and financial services to over 100,000 clients, ranging from small businesses to Fortune 500 companies.

Bambora is a wholly owned subsidiary of Ingenico Group, the global leader in seamless payment. Ingenico Group is a trusted world-class partner for financial institutions and retailers and provides solutions to simplify payments and deliver on their brand promises.

Bambora undergoes a number of rigorous audits and compliance processes and works constantly to protect the privacy and security of customer's data. These include but are not limited to SOC 1 Type 2, CSAE 3416, ISAE 3402, and SOC 2 Type 2. As part of our agreement with our banking and processing partners, we are audited directly on a regular basis.

As a card processing gateway, we comply with and are certified annually as a Level 1 PCI compliant agent. We voluntarily register with the various payment network's third-party agent programs andadopt the newest PCI-DSS versions in order to ensure our systems are secure.

When it comes to the privacy of our customer's, and their customer's data, we follow Generally Accepted Privacy Principles (GAPP), and comply with all privacy laws and regulations in the different regions that we operate in, including but not limited to:

- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- The Gramm-Leach-Bliley Act which is also known as the Financial Modernization Act of 1999
- California Consumer Privacy Act of 2018 (CCPA)

A critical component of our agreement with our banking partners is that we adhere to their level or above in terms of privacy or security.

In the following pages, you'll find answers to some of the commonly asked questions relating to our compliance and security policies. You can also always find the most up-to-date information on our website at https://www.bambora.com/en/ca/.

Security

What security standards does Bambora follow?

Bambora is a worldwide platform, which means we must comply with privacy and data security legislation across many jurisdictions, as well as complying with payment industry requirements.

Bambora follows recommended best practices from public bodies such as CIS (Center for Internet Security), non-profits such as the SANS Institute, as well as various manufacturers in the form of white papers and best practice documentation. These standards are updated constantly to reflect changes to the industry, emerging threats, technological advancements, and changes to our hardware and software selection.

Bambora also follows best practices for development and testing processes and has adopted a number of key requirements from frameworks, such as the Microsoft Security Development Lifecycle and the Agile Security Manifesto, when building out our internal methodology.

What is PCI DSS, and does it apply to me?

PCI-DSS stands for "Payment Card Industry Data Security Standard" and is the global security standardfor companies that handle branded credit cards. Any company that works with credit cards must comply with PCI-DSS in order to be allowed to remain active, from the issuing banks, to the major processing companies, to shopping carts, all the way down to the individual merchants.

PCI DSS includes the following 12 requirements:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

As a credit card gateway and third-party agent, Bambora is classified as a "Level 1 Service Provider", meaning that we have to comply with the most rigorous and detailed version of this security standard. We are required to go through an annual on-site audit from a third-party Qualified Security Assessor (QSA), and then provide a completed Report on Compliance to our banking and processing partners.

Although PCI DSS is used primarily to protect the handling of payment credit card data, because it is such a broadly accepted set of standards there is a huge benefit for all of our clients that Bambora is compliant. All of the services we provide to all of our merchants will touch parts of this process, so we make sure that everything we do is up to this very high standard.

For more details on the standard and benefits of PCI Security Standards Council visit https://www.pcisecuritystandards.org/.

What type of technology does Bambora use?

Bambora takes a layered approach to security, utilizing numerous redundant systems to ensure the confidentiality, integrity, and availability of data and systems, in many cases going beyond what is required by PCI DSS.

Systems are monitored, maintained, and updated rigorously, paying attention to emerging cyber threats and changes in the security landscape.

All of Bambora's web portals that allow user access, or public APIs (Application Programming Interface), support strong encryption technologies. We routinely test our web pages against all current browsers, as well as several older versions of each to guarantee compatibility.

How does Bambora protect my data?

Bambora uses a number of encryption methods, making use of public and private key technologies, one-way encryption (hashing), and both destructive and non-destructive masking to ensure data is not accessed by unauthorized individuals.

How do I ensure that Bambora, as our supplier, meets our security requirements?

In addition to our mandatory PCI assessment and internal audits, Bambora completes a number of voluntary financial and security audits of its systems and processes on an annual basis. These reports may be available to existing merchants who are undergoing their own audits.

- SOC 1 Type II (available to merchants or under a signed Non-disclosure Agreement)
- ISAE3402 (available to merchants or under a signed Non-disclosure Agreement)
- CSAE3416 (available to merchants or under a signed Non-disclosure Agreement)
- SOC 2 Type II (available to merchants or under a signed Non-disclosure Agreement)

Can we perform our own risk assessment audit on Bambora?

Unfortunately, Bambora is not able to accommodate client audits of its operations. As we are audited directly by banks and service partners and perform a number of our own audits, supporting this would be a duplication of efforts. In some situations, we can share the results of our audits with clients in orderto satisfy their own auditing efforts, when it would be appropriate to do so.

Does Bambora provide any cloud-based solutions?

Bambora does not provide any hosting services, including cloud-based solutions. The services weprovide are built in-house and are limited to process of payments or identity verification.

Privacy

What happens with my information, or my customer's information?

We collect personal information directly from you, indirectly from third parties and otherwise as permitted by applicable law. Bambora limits the information we collect about our customers and potential customers to what we need for internal business purposes only.

In order to process payments, either through credit cards or bank transfers, Bambora needs a certain amount of information that you would supply on your application for service or through a "transaction" request. Depending on the service being used, this information may include:

- Name
- Email Address
- Phone Number
- Address
- Credit Card Information
- Bank Information
- Amount being processed

This information is stored securely, and if necessary encrypted, in our system, and accessed only when being processed with our banking partners or in some cases when being used in a report. When Bambora sends the information to our banking partners it's done through direct connections using proper encryption, and access to these services and systems is restricted and monitored at all times.

Where is the information stored?

Personal information that we collect or that is provided to us is stored in Canada on our on-premises data centers and with AWS Cloud Services located in Canada. Where you request us to process a transaction on your behalf, your personal information is transferred to our third-party banking partners, who may process your personal information outside of Canada. Where this is the case, we will take steps to ensure that appropriate safeguards and security measures are in place so that your privacy rights continue to be protected as set out in this privacy policy.

While currently Worldline operates its Canadian platform strictly from Canada data centers, there is a possibility this will change in the near future where systems might also be operated from Worldline's owned data center in the US as well as in Canada. In the occurrence of this change, affected customers will be notified via email.

What if I'm not located in Canada, is my information still protected?

Bambora currently operates in three regions: Canada, the United States of America, and Europe. We have banking relationships in all three regions, and part of those agreements require us to comply with the appropriate banking and privacy legislations in each region.

We store our data in Canada, as the relevant privacy law here is PIPEDA (Personal Information Protection and Electronic Documents Act) and is accepted in Europe as providing "adequate protection"of personal information.

Additionally, Bambora complies with "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", more commonly known as "GDPR", which deal exclusively with data privacy and handling in Europe.

In the United States Bambora complies with the GLBA (Gramm-Leach-Bliley Act) which is also known as the Financial Modernization Act of 1999 and covers handling of private information by financial institutions. For a California resident, Bambora complies with the California Consumer Privacy Act(CCPA), which gives certain rights with respect to the processing of their data.

Is Bambora a Data Processor or a Data Controller?

As Bambora is acting as software between our clients and the various payment processing networks (i.e., Visa, Master Card, ACH, SEPA, etc.) we qualify as a Data Processor. We provide the method and technology to collect and transfer personal data to the networks, but we do not determine the purpose the data is collected for or which individuals to collect the data from.

As a Data Processor Bambora will comply with all applicable requirements of the different data protection regulations including:

- Using appropriate security measures to protect sensitive data
- Having a contract to govern the duration, nature, and purpose of the processing
- Having a designated Data Protection Officer
- Following breach notification rules to alert the Data Controller without undue delay in case of a breach, and assisting the Data Controller in complying with its obligations as appropriate

The Bambora Terms and Conditions speak to GDPR in detail and include a Data Processing Agreement between Bambora and our clients that will apply to any processing covered by GDPR.

What if the laws change, how does that impact my information?

Bambora has agreements in place with banks in every region that we operate in, as well as many third-party processors and merchant account acquirers, all of whom require that we comply with privacy laws in those regions. We actively work with our partners and our global and domestic legal teams to make sure we're aware of any upcoming changes to privacy laws that would impact our services, and if necessary, will make changes to comply with those laws.

Bambora will continue to review its privacy policy to ensure it remains current with changing laws and regulations while meeting the evolving needs of customers. In the event of any amendment to the privacy policy, an email will be sent, and a notice will be posted within this page. If you continue to use our services or websites following an amendment to the privacy policy, you will be deemed to have consented to the updated privacy policy.

How long does Bambora keep my information?

How long Bambora retains customer information depends on the type of information and why it was provided to us. We will retain your personal information for as long as is necessary in order to manage our relationship with you, fulfill the purposes for which it was collected or as necessary or as permitted or required by law.

Currently we retain payment processing information, such as amounts and bank data, for up to two years and one month (total of 25 months), at which point it is permanently deleted from our system. This information is used both for processing the payment as well as reporting and reconciliation, and in the case of errors or disputes with banks it is used help assist the investigation of the payment.

Business information provided during the setup and boarding process will in most cases be retained for the lifetime of the agreement with Bambora, plus up to seven years beyond the termination of the agreement. This information is used as part of our required audits, showing that accounts are setup in accordance with our partner and bank agreements. In some cases, it is also for future internal compliance reviews.

In all cases we may be required to retain data for a longer period of time depending on applicable law or by court order, and clients have the option upon termination of the agreement with Bambora to ask us to destroy all of the non-payment related information considered confidential in nature.

Compliance/Audits

What audits does Bambora go through, and how often?

Bambora goes through several audits (including our security-based audits), with two annual audits that report on both financial and non-financial controls. Bambora performs an audit each year and produces two Service Organization Controls SOC 1 Type 2 report as well as a SOC 2 Type 2 audit report. These two audit reports review the previous year and help to provide information on controls in place and the effectiveness of them.

What does "SOC" mean, and why does it matter?

SOC stands for Service Organization Controls and are a series of standards designed to help measurehow well we as an organization controls our information. There are various levels of reporting frameworks within SOC, and different types of some of these levels as well.

A SOC 1 report has to do with financial reporting controls, with Type 1 providing an explanation on the design of controls and a Type 2 providing additional detail on the effectiveness of the controls. Bambora goes through a Type 2 report, meaning we audit both the presence of appropriate controls and their effectiveness over the audit period being reported on.

A SOC 2 report usually has to do with controls for security, availability, processing, integrity, and privacy. This is a more detailed report and usually contains information around the architecture and processes in place within an organization and goes through how information is protected both on a platform and within the organization itself. It can be used for internal audits as well as for external/partner audits (such as for a PCI audit), and Bambora goes through the Type 2 reporting process.

Both of these types of reports are standard within the financial and payments processing industry in North America and are used to provide details to partners and auditors.

Can you send me copies of your SOC reports?

SOC reports are used expressly for auditing purposes, and generally contain confidential information about an organization. Part of the controls within an organization would be limiting access to the reports themselves and tracking in detail how the reports are given out and used external to the organization.

Bambora is happy to provide as much information as reasonably necessary to clients to help them understand our position on security and privacy but cannot provide full copies of our reports withoutdue process.

If you have any questions or need more information, please reach out to your Account Manager.