

GUIDELINES APPLICABLE FOR GOVERNMENT & LAW ENFORCEMENT

These guidelines outline how government and law enforcement agencies may request information from JB concerning user activity, in accordance with applicable laws. JB reserves the right to update these guidelines as necessary.

For all general inquiries, including data subjects' access requests, please refer to our Privacy Policy or contact our compliance team directly at legal@JB.com.

JB responds to official law enforcement requests in compliance with Curaçao law and applicable international standards. Except in emergency situations, JB will only disclose information pursuant to a valid legal process such as:

- A search warrant issued on probable cause;
- A lawful subpoena; or
- Verified user consent.

All such requests are reviewed by our legal and compliance teams. Requests that are vague, overly broad, or lacking legal basis will be challenged, narrowed, or rejected.

JB will only provide responses to requests from official agency email domains. Requests from unofficial addresses will not be processed.

All legal documents should clearly identify the subject of inquiry, such as a specific username, registered email address, or wallet ID. Data is only provided to the extent that it is retained and accessible in accordance with JB's data retention policies.

Data is retained only for the period necessary for regulatory and business purposes. Requests should be as specific and time-bound as possible to facilitate timely processing.

Customer content (e.g., communication logs, account activity) will only be disclosed with a valid search warrant issued upon probable cause, or as otherwise required by law.

How to Serve Legal Process. Government, Law Enforcement, and Private Party Subpoenas, Search Warrants, and Court Orders

JB accepts service of legal process by email at legal@JB.com. Submissions must originate from an official government or law enforcement domain. Requests submitted through other channels will not be reviewed.

JB will not download legal process documents through any links provided in an email due to system security standards. Additionally, providing a link to download the legal process will not be considered valid service of process. For data security purposes, the complete legal process should be transmitted in password-protected documents and the password transmitted in a separate email.

When government or law enforcement serve legal process on JB by email to legal@JB.com, there is no need to serve a paper copy by mail.

Managing and Responding to Government, Law Enforcement, and Private Party Subpoenas, Search Warrants, and Court Orders.

JB carefully reviews all legal requests to ensure that there's a valid legal basis for each request, and complies with legally valid requests. Where JB determines that there is no valid legal basis or where a request is considered to be unclear, inappropriate or over-broad, JB will object, challenge, reject or ignore the request.

Witness Testimony Subpoenas

JB will not waive service requirements for subpoenas seeking witness testimony nor accept service via electronic means. All subpoenas seeking witness testimony must either be personally served on JB or served through JB registered agent for service of process. JB will resist subpoenas for witness testimony that are served with fewer than 14 days advance notice.

Preservation Requests

Requests to preserve information should be transmitted directly from an official government or law enforcement email address to legal@JB.com. Preservation requests must include the relevant JB user ID/account email address, or full name and physical address of the customer of the subject JB account.

When a preservation request has been received, JB will preserve a one-time data pull of the requested existing customer data available at the time of the request for 90 days. After this 90 day period, the preservation will be automatically removed from the storage server. However, this period can be extended for one additional 90-day period upon receipt of a renewed request.

An attempt to serve more than two preservation requests for the same account will result in the second request being treated as a request for an extension of the original preservation, and not a separate preservation of new data. Requests for initiations of new preservations of data should be separately submitted, and must not be combined with requests for extensions of existing preservations.

Emergency Requests

Authorized disclosure of data, including customer content, by JB may be made under certain circumstances as an exception to the requirement that government or law enforcement obtain a search warrant for customer content.

in situations in which the case involves an emergency, JB is permitted, but not required, to voluntarily disclose information, including contents of communications and customer records where JB believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay.

In order to request that JB voluntarily disclose information on an emergency basis, the requesting government or law enforcement officer should include in the title/subject line:

“Emergency Government & Law Enforcement Information Request” and transmit it directly from their official government or law enforcement email address to. If a government or law enforcement agency seeks customer data in response to an Emergency Government & Law Enforcement Information Request, a supervisor for the government or law enforcement agent who submitted the Emergency Government & Law Enforcement Information Request may be contacted and asked to confirm to JB that the emergency request was legitimate.

The government or law enforcement agent who submits the Emergency Government & Law Enforcement Information Request should provide the supervisor's contact information in the request.

Account Restriction/Deletion Requests

If a government or law enforcement agency requests that JB restrict/delete a customer's JB ID, JB requires a court order (often a judgment of conviction or warrant) demonstrating the account to be restricted/deleted was used unlawfully.

JB carefully reviews all requests from government and law enforcement to ensure there's a valid legal basis for each request. In instances where JB determines there is no valid legal basis or where the court order does not demonstrate that the account to be restricted/deleted was used unlawfully, JB will reject/challenge/ignore the request.

Where JB receives a satisfactory court order (often a judgment of conviction or warrant) from government or law enforcement demonstrating that the account to be restricted/deleted was used unlawfully, JB will take the requisite action to restrict/delete the account in compliance with the court order; and advise the requesting agent/party accordingly.

Customer Notice

JB will notify customers when their JB account information is being sought in response to legal process from government or law enforcement, except where providing notice is explicitly prohibited by the legal process itself, by a court order JB receives, by applicable law or where JB, in its sole discretion, believes that providing notice creates a risk of injury or death to an identifiable individual.

After 90 days, JB will provide delayed notice for emergency disclosures except where notice is prohibited by court order or applicable law or where JB, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual.

JB will provide delayed notice after expiration of the non-disclosure period specified in a court order unless JB, in its sole discretion, reasonably believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals or where notice is not applicable to the underlying facts of the case.