

## Apple Pay Regulations

### Article 1. Definitions

1. The following definitions are used in the provisions below:

**Apple Pay:** a digital card service (wallet) offered by Apple that enables the cardholder to store a Digital Card on their Device, allowing contactless payments through NFC, in-app purchases or other electronic payments.

**Digital card:** a digital version of a physical ING Card that the holder has registered for use with Apple Pay.

**ING Card:** a card of one of the following types, made available by ING for use with Apple Pay a) a physical ING Debit Card issued by ING in Belgium

**Card Terms and Conditions:** General Terms and Conditions applicable to the registered ING Card: a) ING Debit Card General Terms and Conditions.

**Apple Pay's General Terms and Conditions (Apple Terms):** the Apple Pay agreement and terms and conditions that include the rights and obligations of Apple and the cardholder with respect to this service.

**Means of access and signature:** personal security credentials on the basis of which the digital cardholder can be identified and payment orders can be signed. More specifically, the Device's unlock codes (access code, fingerprint, facial recognition).

**Personal security credentials:** personal features given by Apple or ING to the payment service user for the purpose of user authentication.

**Device:** a device that meets the Apple Pay system requirements set by Apple, which allows the cardholder to access Apple Pay's services.

**NFC:** Near Field Communication (NFC) is a technology that allows contactless payments by bringing a device containing a Digital Card and equipped with this technology near to an NFC terminal.

**The account holder:** the natural or legal person holding the account(s) to which the ING Card is linked.

**The cardholder:** the natural person in whose name the ING Card underlying the Digital Card was issued.

**The payment order:** any instruction giving instructions to make a payment.

**The payment transaction:** the act consisting of the payment, transfer or withdrawal, irrespective of the commitments between the parties involved in the underlying transaction on which the payment transaction is based.

**The consumer:** the natural person who, in the context of the use of the payment service, acts with a purpose other than their commercial or professional activity.

### 2. Purpose of these Regulations

Apple Pay is a digital card service offered by Apple, which allows the cardholder, by using a Digital card, to make a payment with their Apple Device, in accordance with the Apple Terms.

These Regulations regulate the rights and obligations of the cardholder and/or the account holder and ING in Belgium (the Bank) with regard to registering an ING Card as a Digital card and the use of the ING Card in Apple Pay for the submission of payment orders to the Bank.

## Article 2. Legal Framework

Except if these Regulations deviate from these, the provisions of the Bank's General Regulations, the Special Regulations for Payment Transactions, the Card Terms and Conditions and the ING Banking General Terms and Conditions apply to the registration and use of the Digital Card to initiate payment orders by means of Apple Pay.

## Article 3. Registering the digital card

### 3.1. Access to Apple Pay

In order to use Apple Pay, the cardholder must have an ING Card and register it in Apple Pay as a Digital Card.

To this end, the cardholder must preferably have the ING Banking App, a compatible Device and follow the instructions for the Apple Wallet and/or ING Banking App and hereby accept the applicable Apple Terms and Privacy Policy.

Access, use and maintenance of the Digital Card in the wallet depend on Apple and the cardholder's Internet connection service provider. The bank cannot be responsible for technical errors, malfunctions or defects in the services provided by third parties such as Apple or the service provider. Nor can the bank be held liable if Apple makes changes to Apple Pay or stops Apple Pay.

The registration of an ING Card in the Apple Pay Wallet for a particular Device is also construed as an explicit acceptance of these Regulations.

## Article 4. Use of Digital Card in Apple Pay

The cardholder gives their consent to the execution of a transaction by using the device on which the Digital Card is available and by using the Device's means of access and signature.

- In a physical store, by holding their Device against the payment terminal for contactless payments and then authorising payment via the unlock code available on the device: face, fingerprint, access code.
- Online (app or web) by choosing the Apple Pay Button and then giving permission with the Device's unlock code, i.e. face, fingerprint or access code.

The terms of the means of access and signature for the various Apple Devices are further described in the Apple Terms and the available technical documentation on the Apple Support page.

The account holder irrevocably authorises the Bank to debit their account for the amount of the payment transactions submitted with the Digital Card.

The cardholder and the account holder acknowledge the validity of the payment orders signed through Apple Pay and sent to ING. These signed payment orders constitute valid and sufficient evidence of their agreement with the existence and content of the transaction.

#### Article 5. Limits of Use – Refusal

The Limits of Use of the underlying ING Card also apply to payment with the Digital Card.

ING reserves the right to refuse to execute certain payment transactions. If the bank refuses to execute a payment transaction, the cardholder shall be informed of this as soon as possible and, if possible, of the reasons for refusal. This notification will be given via the merchant's payment terminal, webshop or app.

#### Article 6. Pricing

The bank does not ask for an additional fee for registering a Digital Card in Apple Pay.

#### Article 7. Terms, frequency of communication and content of information

7.1 To enable the cardholder and/or the account holder to track the status of expenditure on the Digital Card and, where applicable, to provide the Bank with the notification provided for in Article 8.2.1° (notification of unauthorised, incorrect or irregular transactions), data on the payment transactions executed with the Digital Card will be made available in line with the agreed terms of the underlying ING Card, at least once a month.

These data include:

- elements allowing the cardholder and/or the account holder to identify any payment made using the Digital Card and, where applicable, the information concerning the beneficiary of the transaction;
- the amount of the payment transaction expressed in the currency in which the current account linked to the underlying ING Card is debited or in the currency used in the payment order;
- the amount of all costs applied to the payment transaction and, where applicable, the breakdown thereof;
- where applicable, the exchange rate used in the payment transaction and the amount of the payment transaction after that currency exchange;
- the debit value date.

The data shall be communicated by means of account statements or in any other manner agreed between the parties and which enables the storage of the data and their identical reproduction.

7.2 Depending on the type of Device, the cardholder can consult the executed Apple Pay payment transactions via the Apple Pay Wallet made available by Apple. This data is made available to Apple by the bank, among others.

7.3 if the cardholder has notified ING of their mobile number, the cardholder, acting as a consumer, will automatically receive SMS messages in relation to the currency exchange rate of cross-border payment transactions initiated with the card, either in the currency of a Member State of the EEA or in GBP. This information service is provided free of charge by ING. The cardholder has the option of cancelling this service by contacting the ING customer service at any time. (02/464 60 04)

Article 8. Respective obligations and responsibilities of the Bank, the cardholder and the account holder

8.1. The cardholder undertakes to:

1° comply with the prudence measures attached to these Regulations and which form a necessary part thereof.

2° use their Digital Card in accordance with the terms and conditions in force at the time of its use and within the limits of use granted to them; more specifically, the cardholder must ensure that they do not exceed the available limit of use.

3° take all reasonable measures to ensure the confidentiality of their means of access and signature – in particular the PIN code – and not to disclose these to third parties, in order to prevent fraudulent use of electronic payment systems.

For example, and more specifically, they may not write down codes or passwords in an easily recognisable manner on an item or document that the holder keeps or carries with the device, or share these with third parties.

For example, the cardholder shall ensure that a third party cannot add a face or fingerprint to the device on which the Digital Card is available.

Non-compliance with this rule constitutes a serious error, without prejudice to the competence of the courts.

4° keep the device in a safe place in order to prevent any abuse by third parties and, for example, not leave it unattended in a vehicle or a space accessible to the public, unless, in the latter case, it is stored in a locked cabinet or drawer. Places to which a large number of people have actual access, without the areas actually being accessible to the public, are considered to be the same thing.

5° remove an old device, which is no longer in personal use, from the configuration of the Apple Pay Wallet.

6° When they are aware of the loss, theft, unlawful use or unauthorised use of the device, or the means of access and signature that enable use of the Digital Card (such as the secret PIN code), they undertake to report it immediately to Card Stop directly: by telephone (7 days a week, 24 hours a day on 70 344 344 or 32 70 344 344 if you are calling from abroad) or by calling the Customer Services department. (+32 2 464 60 04). **The telephone call with Card Stop or with the ING Customer Services department will be recorded automatically. The data thus recorded shall serve as evidence in the event of dispute and shall be kept in accordance with Article 14 (protection of privacy), without prejudice to Articles VI.83 and VII.2(4) of the Belgian Code of Economic Law.**

In these Regulations, "loss" or "theft" means any inadvertent dispossession of the Device. The term "unlawful use" or "unauthorised use" means any unlawful or unauthorised use of the Digital Card and/or the means of access and signature, even if the Device is still in the cardholder's possession.

7° In the event of theft or loss of their device, the cardholder must immediately get the Device blocked via Apple's "Find my" application.

8° report the theft, loss, unlawful use or unauthorised use of the Device and the means of access and signature that enable a transaction with the Digital Card within 24 hours to the local, Belgian or foreign official authorities. If so requested, the cardholder must provide the Bank or Worldline with the proof and references of the complaint or report. The cardholder undertakes to provide the Bank or Worldline with all information necessary for the investigation. However, non-compliance with the obligations of this Article shall not, in itself, be considered as gross negligence.

9° use at all times the most recent version of Apple Pay Wallet application and iOS and a Device that complies with Apple's security requirements and system requirements.

8.2. The account holder has the following obligations:

1° they must inform the Bank of any charge in their account statements for any transaction carried out without their consent, and of any error or irregularity established on said account statements. This notification must be confirmed in writing.

After the information relating to the contested transaction has been provided or made available, any account holder who is aware of an unauthorised or incorrectly executed transaction, which gives rise to a claim, shall only obtain rectification of such transaction by the Bank if they inform it of the transaction in question without delay and no later than thirteen months after the debit date of the transaction, unless the Bank, if applicable, has not provided or made available the information relating to the contested transaction in the agreed manner.

If the notification was not given in writing, the written confirmation referred to in paragraph 1 of this Article may be given by the account holder after the expiry of the aforementioned time limits.

Where the account holder is not a consumer within the meaning of Article 1, the period of thirteen months after the debit date of the transaction shall be limited to two months.

2° they shall bear the loss linked to any unauthorised payment transaction resulting from the use of the lost, stolen or unlawfully used Digital Card up to a maximum of EUR 50, until the notification referred to in Article 8.1.6°, paragraph 1 is given.

However, the account holder shall not bear any loss – and the EUR 50 limit shall not apply – if: - the loss, theft or unlawful use of the Device or the Digital Card could not be detected by the cardholder before payment (in particular in the event of forgery, copying, hacking or skimming etc. of the card data), except if the cardholder and/or the account holder acted fraudulently; - the loss results from an act or omission by an employee or agent of the Bank, Worldline or Apple.

3° they shall bear all losses caused by unauthorised payment transactions until the notification referred to in Article 8.1.6°, paragraph 1 has been given, if these losses are the result of the fact that the cardholder and/or the account holder intentionally or as a result of gross negligence failed to comply with one or more obligations with which they are required to comply pursuant to the

provisions of these regulations. In that case, the limit of 50 EUR referred to in 2° above does not apply.

The non-compliance with the provisions of Clauses 8.1.3° (to take all reasonable measures to protect the confidentiality of the personal security credentials) and 8.1.6°, paragraph 1 (immediately informing the Bank or Card Stop of the loss, theft, unlawful use or unauthorised use of the Device and/or the Digital Card and/or the means by which it can be used) is considered gross negligence, without prejudice to the sovereign discretion of the courts.

In addition, the Bank points out to the account holder that other facts or conduct, whether or not these ensue from the non-performance by the cardholder and/or the account holder of their obligations under these General Terms and Conditions, may be considered gross negligence, depending on the whole of the circumstances in which they occurred or were expressed, whereby, where applicable, the ultimate discretion is vested in the courts.

4° by way of derogation from the provisions of points 2° and 3° above, the account holder will not bear any loss for payment transactions for which no strong customer authentication is required. However, this exception rule does not apply if it is established that the cardholder and/or the account holder acted fraudulently.

5° if the cardholder and/or the account holder has/have acted fraudulently, the account holder must bear the full loss resulting from unauthorised transactions carried out both before and after the notification referred to in Article 8.1.6°, paragraph 1 (regardless of the Bank's obligation to make every effort to prevent any further use of the debit card).

6° the account holder cannot revoke a payment order after the Bank has received this instruction.

All contractual provisions agreed elsewhere with the Bank for this type of transaction, in particular the provisions relating to coverage for overdraft transactions and to any debit balances that the account or accounts used might show, also apply to said transactions.

### 8. 3. The Bank has the following obligations:

1° it shall ensure that appropriate means are available at all times to enable the cardholder to provide the notification referred to in Article 8.1.6°, paragraph 1, and, where appropriate, to request the blocking of their Digital Card if this is still technically possible.

2° it shall take all necessary measures to prevent the use of the Digital Card as soon as it (or Card Stop) has been informed of the loss, theft, misappropriation or any unauthorised use of the Digital Card and/or the means that make its use possible.

3° upon request, it will provide the cardholder and/or the account holder, for eighteen months from the notification referred to in Article 9.1.6°, paragraph 1, with proof that the cardholder has indeed submitted this notification.

4° except in the event of fraud, gross negligence or wilful default on the part of the cardholder and/or the account holder in connection with one or more obligations with which they are required to comply pursuant to Articles 8.1 and 8.3, the Bank shall bear any loss exceeding the amount of EUR 50 charged to the account holder for unauthorised transactions carried out before the notification referred to in Article 8.1.6°, paragraph 1.

5° the Bank shall bear all the loss suffered by the cardholder if:

- the loss, theft or unlawful use of the Digital Card could not be detected by the cardholder before payment (in particular in the event of forgery, copying, hacking or skimming etc. of the card data), except if the cardholder and/or the account holder acted fraudulently;

- the loss results from an act or omission by an employee or agent of the Bank or equensWorldline.

6° except in the event of fraud on the part of the cardholder and/or the account holder, it will bear the losses associated with the unauthorised payment transactions carried out after the notification referred to in Article 8.1.6°, paragraph 1.

7° except in the event of fraud on the part of the cardholder and/or the account holder, it will bear all consequences ensuing from the use of the debit card by an unauthorised third party in the event of non-compliance with one of the obligations referred to in points 1° and 3° of this Article 8.4.

8° unless it has been established that the cardholder and/or the account holder acted fraudulently, it will bear the successive losses of any unauthorised transaction if this transaction did not require strong client authentication.

9° if, in compliance with the provisions of Article 8.3.1°, the account holder disputes that a payment transaction is permitted or alleges that a payment transaction was not executed correctly, the Bank undertakes to demonstrate on the basis of a copy of its internal entries or by means of another relevant element, depending on the circumstances, that the transaction was authenticated, properly registered and booked and that it did not suffer from a technical defect or any other failure.

The transactions executed using the Digital Card are automatically recorded on a journal strip or an information carrier. The Bank, the cardholder and the account holder assign evidentiary value to the journal strip on which the data are registered in respect of all transactions at the cash dispenser or terminal and/or to the information carrier that might replace or supplement this strip. For any transaction at a cash dispenser or payment terminal for which a printed document containing the details of the transaction can be issued, that document has an informative value. The above provisions shall be without prejudice to the right of the cardholder and/or the account holder to provide proof to the contrary by any legal means and shall be without prejudice to mandatory legal provisions or public policy provisions which might lay down special rules on the evidence of electronic transactions carried out using the debit card.

10° the amount of the Bank's contribution in the event of non-executed, incorrect or unauthorised transactions has been determined as follows:

a) for the non-execution or incorrect execution of a payment transaction that took place using the Digital Card, the Bank shall refund the account holder, if necessary and without delay, with the amount of the non-executed or incorrect transaction and will return the debited account to the situation it was in before the incorrect transaction took place. The value date of the crediting shall correspond to the value date of the debiting of the initial transaction. The Bank shall also owe any interest and costs that the account holder may have incurred as a result of the non-execution or incorrect execution of the payment transaction, provided that such interest and costs are supported by documentary evidence. The account holder will only receive the correction of a transaction that has not been executed or has been executed incorrectly if they have submitted their complaint in good time, in accordance with the provisions of Article 8.4.1°.

b) for an unauthorised payment transaction, the Bank shall immediately refund the account holder with the amount of the unauthorised transaction by returning the debited account to the situation it was in before the unauthorised transaction took place. The value date of the crediting shall correspond to the value date of the debiting of the disputed transaction. This provision is without prejudice to the obligations and responsibilities of the cardholder and the account holder as described in Articles 8.1 and 8.2.

c) in the case referred to in 6° (loss, theft or unlawful use of the debit card that could not be detected by the cardholder before payment) and in 8° (use of debit card without strong client authentication) and unless the cardholder and/or the account holder acted fraudulently, the Bank shall refund the account holder without delay with the necessary amount in order to restore the debited account to the situation it was in before the use of the lost, stolen or unlawfully used debit card as referred to in Article 8.2.2°, paragraph 2, and Article 8.3.6° of these General Terms and Conditions, or of the Digital Card used without strong customer authentication, under the correct value date. Apart from the amounts referred to in the previous paragraphs, the Bank must also refund the account holder for any other financial consequences, such as the amount of expenses borne by the account holder to determine the losses to be compensated, provided the amounts claimed pursuant thereto are established using documentary evidence. By way of derogation from the foregoing provisions, the Bank accepts no liability in the event of force majeure or where the Bank is bound by other legal obligations laid down by national laws or by the European Union. Moreover, where the account holder is not a consumer within the meaning of Article 1, the Bank shall only be liable in the event of a non-executed or incorrectly executed transaction if there has been a serious or intentional error in its services. In such a case, its liability shall in every respect be limited to the direct damage suffered and demonstrated by the account holder, excluding any indirect damage, including but not limited to loss of profit, lost business opportunities, lost customers or damage to its reputation.

11° the Bank shall refuse payment orders made with Digital Cards for which the underlying ING Card was not registered in advance.

12° it shall keep an internal register of payment transactions for a period of at least ten years from the execution of the transactions, without prejudice to other statutory provisions regarding the provision of supporting documents.

13° in any event, it accepts the responsibility for any serious or intentional error in its services.

#### Article 9. Blocking Digital Card

9.1. The Bank reserves the right to block the use of the Digital Card for objectively justified reasons relating to the security of the Digital Card or the underlying ING Card or where there is a suspicion of unauthorised or deceptive use of the Digital Card and/or ING Card and/or the means enabling its use.

9.2. Where the Bank exercises its right to block use, it shall inform the cardholder and/or the account holder thereof by letter, by means of a notification on the account statements or in any other manner it deems appropriate in the light of the circumstances, if possible before blocking, and otherwise immediately thereafter, unless the provision of such information is impeded for objectively justified security reasons or prohibited by applicable law.

9.3. Once the reasons justifying the blocking no longer exist, the Bank will unblock the Digital Card.



## Article 10. Duration and end of the contract

10.1. The contract relating to the registration and use of the Digital Card is concluded for an indefinite period.

10.2. The cardholder and/or the account holder may terminate the contract with regard to the provision and use of the Digital Card without any costs or justification and with immediate effect. Cancellation can be effected by removing the Digital Card from the Apple Pay Wallet.

10.3. The Bank may terminate the contract without justification provided that it complies with a notice period of two months, which is communicated by letter (post or registered) or on any other durable medium, for example an e-mail to the last (postal or electronic) address of the cardholder and account holder known to the Bank.

This provision applies without prejudice to mandatory statutory provisions of public policy imposed by the Bank to terminate the contract and/or to take special measures in exceptional circumstances, and without prejudice to Article 10 (right to block the use of the Digital Card).

10.4. The notice period referred to in Article 11.3, paragraph 1 shall not apply if the account holder is not a consumer.

10.5 the termination of the agreement for the underlying ING Card will result in the termination of the agreement on the part of the cardholder by law. at the same time.

The replacement of the ING Card due to theft or loss will result in the automatic termination of the Digital Card agreement. A replacement card will have to be re-registered in accordance with Article [3].

## Article 11. Processing of personal data

The personal data of the account holder or cardholder that are communicated:

- when registering the Digital Card for the use of Apple Pay
- when submitting payment orders by means of Apple Pay

are processed by the Bank in accordance with the Privacy Policy applicable to the ING Card issued by the Bank, which was registered as a Digital Card by the cardholder.

As a result of the use of Apple Pay, Apple also has access to data relating to the card transactions executed through the use of Apple Pay. The Cardholder agrees to Apple's applicable Privacy Policy. The Bank is not a party to the contract between the cardholder and Apple regarding this processing. More information can be found in the Apple Terms and Apple's Privacy Statement.

More information about the processing of personal data by the Bank can be found in:

- Article 14 of the Card Terms and Conditions
- Article 6 (Protection of privacy) of the Bank's General Regulations, and
- the ING Privacy Statement attached as an annex to the aforementioned Regulations.

All data subjects can contact the Bank via the usual means of communication with any questions about the processing of personal data by the Bank:

- by logging in to the ING Banking services and, where appropriate, sending a message via these services with the subject "Privacy",
- by contacting their ING branch or their contact person at the Bank,
- by calling +32 2 464 60 04, - by sending an e-mail to [info@ing.be](mailto:info@ing.be) with the subject "Privacy".

Data subjects may address complaints about the processing of personal data by the Bank to the Bank's Complaint Management service by sending a message with the subject "Privacy", plus a copy of their identity card or passport:

- by letter to the following address: ING Belgium, Complaint Management, Cours St-Michel/Sint-Michielswarande 60, 1040 Brussels;
- by e-mail to the following address: [complaints@ing](mailto:complaints@ing).

Data subjects who are not satisfied or require additional information about the protection of privacy may contact the Bank's Data Protection Officer ("DPO"):

- by letter to the following address: ING Privacy Office, Cours St-Michel/Sint-Michielswarande 60, 1040 Brussels;
- by email to the following address: [ing-bePrivacyOffice@ing.com](mailto:ing-bePrivacyOffice@ing.com)

All data subjects also have the right to lodge a complaint with the supervisory authority competent for the protection of privacy. For Belgium, this is the Data Protection Authority (Drukpersstraat 35, 1000 Brussels; [www.privacycommission.be](http://www.privacycommission.be)).

#### SOME SAFETY TIPS PAY SECURELY WITH YOUR DEVICE/DIGITAL CARD

Your Device (with Digital Card) is a convenient and completely personal instrument!

- Destroy any debit cards whose validity has expired or as soon as you receive a new one.
- Store your Device in a pocket or bag or in a safe place. Never leave it in a place accessible to third parties (for example a sports hall), at your place of work or in your car. Keep your payment receipts. Always check your account statements immediately. If you notice anything out of the ordinary, please contact your bank or the sender of the statement immediately.
- Keep an eye on your device to the extent possible when you pay to a merchant. Make sure that you actually get your own device back after payment.
  - For the sake of ease, you may be inclined to choose one code for all your devices, cards or access codes. Of course, this also entails risks!
- Your secret PIN must remain secret: do not share it with anyone, not even a family member, a friend or someone "in good faith". No one has the right to ask for your code: not your bank or the police or an insurance company.
- Do not write down your secret PIN code, even in encrypted form, for example hidden in a false telephone number.
- Keep your device personal, do not allow anyone to register their face or fingerprint as a means of access and signature for your Device.

- Always key in your secret PIN code or unlock pattern discreetly. Always avoid someone watching you unobserved, for example by shielding the keypad with one hand. Don't let anyone distract you. If you notice anything unusual, please immediately inform your bank branch or, where appropriate, the merchant.

- If you have valid reasons to believe that your secret PIN code is no longer secret, please do not hesitate to change it according to the procedures on your Device. If you are unable to change your code, contact your bank immediately or block your ING Card via Card Stop.

What should you do in the event of loss, theft or any other incident? Immediately notify Card Stop on telephone number + 32 70 344 344 (or the number that your bank issued). This service is available 7 days a week and 24 hours a day and will immediately block your debit card.

If you call from abroad and do not have a touch phone, simply wait until the end of the menu, after which you can speak to an operator. Make a note of the registration number of your call to Card Stop. This will be useful in the later processing of your file. Or notify the Bank by calling the Client Services department +32 2 464 60 04.

In the event of loss or theft of your debit card or device, you must ensure that the local police services draw up an official report within 24 hours and you should ask them for a copy or full reference. Would you like more information? Your bank will be happy to provide you with additional information regarding its own products and services.

Here are a few tips on how to pay safely:

- always store your Device in a bag or pocket or in a safe place.
- your secret PIN must remain secret: do not share it with anyone and do not write it down anywhere.
- always enter your secret PIN code discreetly.
- select a new secret PIN code if you suspect that a third party has taken note of it.
- immediately flag up any irregularity on your account statements.
- in case of loss, theft or any other incident, contact Card Stop (+ 32 70 344 344) immediately. This service is available 7 days a week and 24 hours a day and will immediately block your debit card. Or by calling the Client Services department (+32 2 464 60 04). Make sure you have the Card Stop phone number to hand (for example, in your mobile memory) or learn it off by heart. In case of emergency, you will find it on most terminals.

Apple Pay, Apple Wallet, Apple devices are Apple Inc trademarks: Apple Inc., having its registered office at One Infinite Loop Cupertino, CA 95014, United States.