Personal Cyber Insurance

Terms and Conditions for Visa Infinite & Signature Cardholders in Kuwait

Table of contents

1. What is this document?

The policy pays benefits in accordance with these Terms and Conditions and has been made available to the Eligible Cardholders through the Policyholder.

This document constitutes the full Terms and Conditions of the insurance with Us. Please take time to read these documents carefully to ensure You understand the cover provided.

2. Eligibility

The insurance shall be provided on the condition that the Cardholder:

a) is over 18 years of age and is resident and domiciled in the Territory for the duration of the entire Policy Period; and
b) the Policyholder has paid the required premiums.

3. Important contact information

Make a Claim

Need to make a Claim? Give Us all the details so We can help You out asap (more information later under 'How to make a Claim'). Contact Us at creditcardclaims@crawco.me

Make a complaint

We are dedicated to providing a high quality service and want to maintain this at all times. If You are not happy with Our service, please contact Us, quoting the first 9 digits of your card number and/or claim number, so we can deal with the complaint as soon as possible. Our contact details are:

Warba Insurance Company K.S.C., WARBA Tower - Ahmad Al-Jaber St. Al-Abdulrazzak Sq. Safat, Kuwait City, Al Asimah 13103 Kuwait

In the event that You remain dissatisfied, You can refer the matter to Ministry of Commerce and Industry. Their contact details are:

Ministry of Commerce and Industry

Ministerial Complex, Mergap

P.O. Box 2944 Safat, Kuwait City - 13030, Kuwait

Phone : +965-22480000

Fax : +965-22451080

Email : suad@moci.gov.kw

Website: http://www.moci.gov.kw

Table of contents

4. Summary of benefits

Here is a summary of the insurance benefits:

Insurance Benefit	Cover	**Annual Aggregate Limit**	**Per Occurrence Limit**	Excess
Social Engineering	In the event You are a victim of a Social Engineering Attack and funds have been transferred by You, or in the event You are a victim of OTP Fraud, We will reimburse you for the loss You have suffered.	$2,000 for a Social Engineering Attack $750 for OTP Fraud (limited to 1 Claim per card)	$1,000	$50
Online Shopping Fraud	In the event You made an online purchase, but You subsequently discover the website to be fraudulent, We will reimburse You for that loss.	$2,000	$1,000	$50
Cyber Security Portal	You will have access to an online portal which provides You with a 'Personal Cyber Security Score' and tools to help You stay safe online, including monitoring of 2 email addresses, 3 devices, 2 phone numbers and 2 credit cards.	n/a	n/a	n/a

For full details of Your insurance benefits, including what is and is not covered, please refer to sections A to C of section 8. 'What is insured?'

5. Law applicable to your policy

This policy, and any non-contractual obligation arising out of or in connection with it, will be governed by and construed in accordance with the laws of the Territory. Any dispute will be subject to the jurisdiction of the competent courts of the Territory.

6. Assignment

This policy may not be assigned by You or the Policyholder, and We will not be bound to accept or be affected by any notice or any trust, charge, lien, purported assignment, or other dealing with or relating to this policy.

Glossary of terms

7. Definitions

Here is the lexicon of the terminology we use throughout this document, when capitalised:

Annual Aggregate Limit means the maximum amount per Cardholder for which the Insurer is liable during the Policy Period.

Business Account means any bank account or E-money Account connected to a business and which is not used in a personal capacity.

Cardholder(s) mean all individuals who have been issued an Eligible Card, including secondary or additional cardholders on the same account, in the Territory where such Eligible Card is issued by a participating Issuer.

Insurer / We / Us / Our means Warba Insurance Company K.S.C., WARBA Tower - Ahmad Al-Jaber St. Al-Abdulrazzak Sq. Safat, Kuwait City, Al Asimah 13103 Kuwait.

Claim means a request by You following a loss for any of the entitlements and benefits under this policy.

Digital Content(s) means data that is produced and supplied in a digital form. Examples of this include, but are not limited to software, games, apps, ringtones, e-books, online journals, and digital media such as music, film and television. Digital contents may be supplied to You in a tangible form (for example disk or pen drives), or intangible form such as downloaded, streamed or accessed on the web.

E-money Account means an account provided to You by the Issuer to store electronic money (e-money) online that is accessible through Electronic Device(s).

Electronic Device(s) means any personal network connected devices including, but not limited to desktop computer, laptop/notebook, smartphone, tablets, personal organiser, and router(s) which are not associated or connected to your business, if applicable.

Electronic Transaction(s) means paying using an Eligible Card or E-money Account.

Eligible Card(s) means Infinite & Signature cards issued within the Territory.

Eligible Cardholder(s) means those Cardholders with Eligible Cards that are valid, open and in good standing (not cancelled, suspended or delinquent) at the time of Claim who shall be entitled to receive payment or such other benefit as is provided for in this Policy.

Eligible Item(s)/Service(s) means an any items, services or Digital Contents which are:

1. Not counterfeit or fake goods.
2. Not stocks, shares, bonds, currencies, or digital assets.
3. Not goods bought using store credit or finance/leasing options, or which were not paid in full.
4. Not goods purchased from a natural person through a private transaction.
5. Not confiscated or declared illegal by any government, customs, or public body.
6. Not animals or livestock.
7. Not jewellery, watches, firearms, precious metals/gemstones, art, antiques, or collectable items.
8. Not cash or its equivalents, traveller's cheques, or tickets.
9. Not classified as real estate.
10. Not motor vehicles, motorcycles/scooters, watercraft or aircraft and any equipment and or parts necessary for their operation or maintenance.
11. Not subscription based where You are paying a monthly fee for the services.

Excess means the amount payable by You towards each successful Claim, where applicable.

Glossary of terms

Family means Your spouse, partner or parents or Your children, brothers and sisters including stepbrothers/stepsisters and children who permanently reside with You at the address registered with Us.

Policyholder means Visa International Service Association (Visa) of 900 Metro Center Boulevard, Foster City, California 94404, USA.

Identity Theft means the theft of personal data or documents relating to Your identity which results in You:

1. having money taken fraudulently from Your E-money Account, bank or building society; and/or
2. being held liable for payment of goods or services purchased or contracted fraudulently by others.

Issuer means a Bank or financial institution or like entity that is authorized by Visa to operate a Visa credit or debit card program in the Territory and is participating in this policy offering to Eligible Cardholders.

Mass Cyber-Attack means an act intended to affect multiple persons due to any kind of single system-wide failure, malware, theft, misuse, mishandling and/or data hack of any data and/or databases and/or other forms of storage under the control of private and public sector organisations (including the Policyholder or any of its affiliates and/or subsidiaries) for which they are responsible and/or liable and/or have relevant corporate insurance protection in place.

OTP Fraud means someone convinces You to reveal Your one-time passcode (OTP), enabling them to fraudulently access the funds in Your bank account or E-money Account.

Per Occurrence Limit means the maximum amount of benefit payable under the policy for any single covered loss occurrence.

Policy Period means 1st September 2024 to 31st May 2025.

Proof of Purchase means the original purchase receipt that has details of Your items. If this is not available, then other evidence which clearly demonstrates Your ownership of the items.

Retailer / Seller means a trade registered company that sells goods direct to consumers (not to businesses) in stores and/or on the internet, including e-commerce platforms through which third party merchants sell their goods.

Social Engineering Attack means attacks that are carried out to trick You into opening or responding to emails, text messages, phone calls and websites that appear to be from legitimate entities or people who You trust and/or are known to You with the purpose of convincing You to transfer funds. Examples of such scams include but are not limited to: Phishing (emails); Smishing (text messages); Vishing (fraudulent pre-recorded messages); Spoofing (impersonation phone calls).

Territory means Kuwait where the Cardholder legally resides, and where an Eligible Card is issued by a participating Issuer.

Theft / Stolen means taking Your property without Your permission with the intention of permanently depriving You of it.

Third party means anyone other than You or Your Family members.

You means the Eligible Cardholder and beneficiary of the insurance coverage.

Your means belonging or pertaining to You.

Cover

8. What is insured?

The following Cover sections of this document provide full details of Your insurance cover, including:

- What is covered under each specific insurance coverage.
- What is **NOT** covered under each specific insurance coverage.
- What to do in the event of a Claim under each specific insurance coverage.
- If an Excess is applicable to the insurance coverage.

Section A: Social Engineering

In the event You are a victim of a Social Engineering Attack requesting You to transfer funds from Your personal account linked to Your Eligible Card(s) to the account of a Third Party and You transfer funds as a direct result of such request; or in the event You are a victim of OTP Fraud whereby a Third Party fraudulently gains access to the funds in Your account, We will reimburse You up to the limits stated in section 4. summary of benefits.

In the event You are a victim of a Social Engineering Attack or OTP Fraud:

1. You must report the fraud to the relevant police authority in the Territory within 24 hours of You discovering it. You will need to obtain a crime reference number.
2. You must notify Your bank or Your E-money Account provider within 24 hours of You discovering the fraud, so it can make attempts to stop the transaction from going through or to trace where the funds have gone.
3. You must notify Us as soon as You become aware You have been a victim of a Social Engineering Attack or OTP Fraud, and no later than 30 days from the date you first discovered you were a victim of this fraud.
4. You must be able to demonstrate that You have taken reasonable steps to:
    a. authenticate and verify the identity of the person who sought to obtain the funds from You.
    b. that the person was entitled to receive payment.

Reasonable steps to verify the identity of the person who sought to obtain funds from You may include, but is not limited to:

- contacting the person via an alternative communication channel and asking them directly if they requested the money; and/or
- verifying with the bank that the provided payee information is legitimate/matches their records.

We understand in some instances Your bank or E-money Account provider may reimburse You for these transactions, but if Your bank or E-money Account provider has refused to accept liability in writing and You have complied with the terms and conditions of Your bank or E-money Account provider, and complied with the terms and conditions of this Policy, then We will reimburse You for these transactions.

What is NOT insured under Social Engineering:

- any transfer from a Business Account.
- any advance fee fraud where You are promised goods, services and/or financial gains, in return for an upfront payment including payment by Electronic Transaction(s).
- confidence/romance scams, where someone befriends You, forms a personal connection with You, or pretends to be interested in a romantic relationship with You and convinces You to transfer money to them.
- any transactions made by Family members, or someone known to You.

Excess applicable to Social Engineering:

An Excess will be deducted for each successful Claim. The Excess due is shown in section 4. summary of benefits.

Section B: Online Shopping Fraud

You are provided indemnity when You discover You have purchased an Eligible Item(s)/Service(s) online from a Third Party for personal use, but the Seller's website/trading platform turns out to be fraudulent. The payment for these Eligible Item(s)/Service(s) must have been completed using Your Eligible Card(s) or account linked to Your Eligible Card(s).

Please note: The intention of this cover is not to indemnify You for online transactions which are completed on genuine websites/trading platforms, where the legitimate Seller:

- becomes insolvent; and/or
- fails to deliver the Eligible Item(s)/Service(s); and/or
- the Eligible Item(s)/Service(s) are delivered damaged or faulty.

In the above circumstances, You should raise Your issue with the online vendor or refer to the consumer law/rights that protect You in the Territory.

In the event You are a victim of Online Shopping Fraud:

1. You must report the fraud to the relevant police authority in the Territory within 24 hours of You discovering it. You will need to obtain a crime reference number.
2. You must notify Us as soon as You become aware You have been a victim of this fraud, and no later than 30 days from the date you first discovered you were a victim of this fraud.
3. You must demonstrate that You have made reasonable attempts to contact the Seller to seek recovery or refund of Your online purchase.
4. You must notify Your Eligible Card issuer/bank or Your E-money Account provider within 24 hours of You discovering this fraud to minimise further losses from this fraud.

We understand in some instances Your Eligible Card Issuer/bank or E-money Account provider may reimburse You for these transactions, but if Your Eligible Card Issuer/bank or E-money Account provider has refused to accept liability in writing and You have complied with the terms and conditions of Your Eligible Card Issuer/bank or E-money Account provider, and complied with the terms and conditions of this Policy, then We will reimburse You for these transactions.

What is NOT insured under Online Shopping Fraud:

- online purchases where cash, crypto currency such as bitcoins, voucher or reward point is the form of payment.
- unauthorised transactions on Your Eligible Card or E-money Account because of this fraud leading to the cloning of Your Eligible Card or Identity Theft.

Excess applicable to Online Shopping Fraud:

An Excess will be deducted for each successful Claim. The Excess due is shown in section 4. summary of benefits.

Section C: Cyber Security Portal

During the period of Your policy, You are provided access to a cyber security portal, which provides You with a "Personal Cyber Security Score" and reports to help You stay safe online. The portal will assess over 70 risk factors to

determine Your cyber security score, which will enable You to understand Your digital footprint and ways in which Your information, money or privacy may be at risk of compromise.

You will be provided with:

- Monitoring up to two [2] personal email addresses, two [2] credit cards and two [2] phone numbers of Yours
- Device vulnerability protection for three [3] Electronic Device(s)
- Router vulnerability protection
- Scam prevention training and alerts

To register for this benefit, please visit https://gcc.dynarisk.com/en_GB/signup/kuwait where you will find instructions on how to login and activate the cyber security portal.

9. General terms and conditions

General Conditions

These conditions apply to all coverages of this policy:

- We have no duty to provide coverage under this policy unless there has been full compliance with Your obligations as set out in this policy.
- You must take reasonable steps to avoid losses.
- For each of the benefits, regardless of the number of Claims made individually or in aggregate, We will pay up to the maximum amount as shown in section 4. summary of benefits.
- You must not agree to limit or exclude any right of recovery You may have against a Third Party for loss, damage or liability that is or may be subject to a Claim under this cover.
- You agree that We have the right to pursue Your rights of recovery against a Third party (where permitted by law) for loss, damage or liability that is or is likely to be subject to a Claim under this cover and You must do everything reasonably necessary to assist Us to do so.
- You must be a resident of the Territory at the time of application for this insurance and remain a resident of the Territory during the term of this policy. If You are planning to move to another country outside the Territory, You must contact Us to see if this policy can remain in force.

General Exclusions

These exclusions apply to all coverages on this policy. We do not provide cover for:

- any incident prior to the start date of Your insurance policy or after the cancellation.
- any losses made on Your Eligible Card or E-money Account more than two (2) months prior to You first reporting the incident to the Eligible Card Issuer and relevant authorities.
- the first amount of every successful Claim (the Excess), wherever applicable.
- any losses which are recoverable from any other source such as but not limited to Your bank, Your E-money Account provider or third-party payment platforms.
- any loss before or after the incident, if You have wilfully concealed or misrepresented any material fact or circumstance concerning this insurance or provided fraudulent information to Us.
- any loss resulting from war, invasion, act of foreign enemy hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection or military or usurped power, nationalisation, confiscation, requisition, seizure or destruction by the government or any public authority.
- any loss resulting from gambling, lottery, contest, promotional game, or other games of chance.
- any loss resulting from illegal activity engaged in by You whether knowingly or unknowingly.
- any loss caused intentionally by You, or Your Family members.
- any loss resulting from a potential Mass Cyber-Attack.

Claims

10. How to make a Claim

When making a Claim, You must:

1. Contact the Cyber Claims Support team by email at creditcardclaims@crawco.me
2. Provide the following information:
    i. Your name.
    ii. The first 9 digits of Your covered card number.
    iii. Your address.
    iv. The section of cover under which You wish to make a Claim.
3. Provide all Your original invoices, receipts, reports (including crime reference number where applicable) and any other documentation necessary to support Your Claim.
4. Provide Proof of Purchase for items being claimed, where applicable. If no Proof of Purchase can be provided Your Claim may not be paid, and this decision will be made at Our discretion.

All information and evidence required by Us shall be furnished at Your expense and shall be in such form and nature as We may prescribe to process the Claim.

If You fail to comply with the Terms and Conditions of this cover, We may be entitled to refuse to pay or reduce the Claim amount payable.

Please first read the relevant sections of the specific benefits and the section entitled 'General Terms and Conditions' to determine what is covered, noting particularly conditions and exclusions and/or requests for specific data relating to Your Claim.

We will make payments within thirty [30] days of the Claim being approved by Us.

11. Fraudulent Claims

If You, or anyone acting on Your behalf, knowingly makes a Claim which is in anyway dishonest, false, or fraudulent, this policy will become invalid. This means that We will not pay the Claim, or any subsequent Claim and may give notice to cancel this policy from the moment that the dishonesty, falsehood, or fraud occurred. In addition, We may recover amounts We have already paid in respect of the Claim.

In the event of dishonesty, falsehood or attempted or actual fraud, Your details may be shared with relevant insurance industry databases and law enforcement authorities, and this may result in future insurance being denied and You may be prosecuted.

Changes and complaints

12. Changes to the policy

The Policyholder may, during the period of insurance, add or delete Cardholders from this policy through declarations. The Policyholder may not make changes to this policy except where specifically agreed in writing by Us.

We reserve the right to make changes to or add to the policy terms applicable:

- for legal, regulatory or taxation reasons; and/or
- to reflect new industry guidance and codes of practice; and/or
- to reflect legitimate cost increases or reductions associated with providing this policy.

If this happens, We will write to the Policyholder with details of the changes at least ninety [90] days before We make them. It is the Policyholder's responsibility to inform Cardholders of such changes. Any changes We make will be the same for all Cardholders under the policy. We will not make changes that apply only to a particular Cardholder, other than that stated in part b) of section 13. Cancelling the policy.

13. Cancelling the policy

We may cancel:

a) this policy by giving ninety [90] days' written notice to the Policyholder at their last known address. In the event of cancellation by Us the Policyholder must notify all Cardholders of such cancellation.
b) Your cover, if You have knowingly provided incomplete, false, or misleading information that We have asked for during the policy application process, at any time during the period of insurance, or in respect of a Claim.

Regulatory statements

14. Data privacy statement

The Personal Information

Warba Insurance Company K.S.C. is the data controller and We accept fully Our responsibility to protect the privacy of customers and the confidentiality and security of Personal Information entrusted to Us.

In this notice, where We refer to Personal Information, this means any information that identifies an individual and includes any sensitive Personal Information (e.g. information about health or medical condition(s)). Where We refer to 'You' or

'Your' Personal Information, this will include any information that identifies another person whose information You have provided to Us (as We will assume that they have appointed You to act for them). You agree to receive on their behalf any data protection notices from Us.

We will use Your Personal Information for the purpose of providing insurance services. By providing Personal Information, You consent that Your Personal Information, will be used by Us, Our group companies*, Our reinsurers, Our service providers/ business partners, and Our agents for administration, customer service, claims handling, assistance services, customer profiling, and for management and audit of Our business operations. We may also pass Your Personal Information to other insurers and regulatory and law enforcement bodies for the prevention of fraud, financial crime or where the law requires us to do so.

We will not share Your sensitive Personal Information unless We have either specific consent from You or Your nominated personal representative or We are required to do so by law. We may transfer Your Personal Information to other countries which may not have the same level of data protection as your home country, but if We do, We will ensure appropriate safeguards are put in place to protect Your Personal Information.

For questions regarding Your Personal Information, please contact:

Warba Insurance Company K.S.C., WARBA Tower - Ahmad Al-Jaber St. Al-Abdulrazzak Sq. Safat, Kuwait City, Al Asimah 13103 Kuwait.

15. Sanctions

No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose the (re)insurer, to any sanction, prohibition or restriction implemented pursuant to resolutions of the United Nations or the trade and economic sanctions, laws, regulations or restrictions of the European Union, United Kingdom, the United Arab of Emirates, the DIFC, the Kingdom of Bahrain, the Kingdom of Saudi Arabia, the Arab Republic of Egypt or United States of America.