Personal Cyber Insurance

an post insurance

Policy booklet

Welcome

Personal Cyber Insurance

Thank you for choosing An Post Insurance Personal Cyber Insurance which is arranged, administered and underwritten by Chubb European Group SE.

This document together with the Policy Schedule 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 and check that **your** details included in the Policy Schedule are correct. **You** should notify **us** immediately if anything is incorrect, as this could affect **your** cover in the event of a **claim**. **We** recommend **you** keep the documents in a safe place, so they are available should **you** need to make a **claim**. **You** should review **your** cover regularly to ensure it continues to meet **your** needs and notify **us** if any of **your** information changes (e.g. change of name or address etc), as this could affect the ongoing administration of **your** Policy or in the event of a **claim**.

These Terms and Conditions explain the nature of the insurance arrangement, the benefits provided, and the risks covered.

This policy meets the demands and needs of customers wishing to protect themselves in the event of being the victim of various types of cyber fraud, **cyber-attacks**, or cyber bullying.

Jim Duncan
Authorised Official
For Chubb European Group SE

Contents

Information

Customer Services

T 1800 320 320
Call this number if your circumstances change and you need to update your policy or if you wish to cancel the insurance. Opening Hours 9am to 5pm Monday to Friday.

Cyber Helpline & Claims

T +353 (0)1 440 1748

Opening Hours 9am to 5pm Monday to Friday.

Insurer

Chubb European Group SE trading as Chubb, Chubb Bermuda International and Combined Insurance, is authorised by the Autorité de contrôle prudentiel et de résolution (ACPR) in France and is regulated by the Central Bank of Ireland for conduct of business rules.

1. Eligibility of Benefits under this Policy

Important: To be eligible for this cover **you** must be 18 or over and a resident of the Republic of Ireland. The coverage and benefits as described in these Terms and Conditions **you** are entitled to, are shown in the Policy Schedule.

2. Summary of Benefits and Scope of Cover

The table below provides a summary of the benefits provided pursuant to the Terms and Conditions set out in this document. The **Excess** and limits applicable under each section are shown in **your** Policy Schedule.

Section	Benefit	Cover	Page
A	Online Shopping Fraud	In the event **you** have completed an **electronic transaction** to purchase **eligible items/services** online including **digital contents** from a **third party,** but **you** subsequently discover the website to be fraudulent **we** will reimburse **you** for that loss.	9
B	Cyber Extortion	In the event **you** are a victim of a **cyber extortion attack, we** will provide **you** with technical support. If the attack can be stopped without paying the extortion amount, then **we** will provide indemnification up to the value stated in the Policy Schedule to restore **your electronic device(s).** If it becomes apparent the extortion amount needs to be paid to unlock **your electronic device(s),** then **we** will indemnify for the amount **you** pay up to the value stated in the Policy Schedule, subject to approval from **us** and compliance with **our** sanctions wording in section 14 of this document.	10
C	Identity Theft	In the event **your** identity has been stolen, **you** are provided with indemnity for legal expenses to engage with a legal adviser to restore **your** identity and any loss of income.	11
D	Cyber Bullying	In the event **you** are a victim of **cyber harassment** or there is a serious and malicious **breach of your privacy** online, **you** are provided cover to seek professional advice and assistance from **your** chosen legal advisers up to the value stated in the Policy Schedule to assist **you** in seeking to have the contents removed and to prevent further harassment.	12
E	Hacker Damage	In the event **your** insured **electronic device(s)** is **hacked** during a **cyber-attack**, **we** will provide indemnification up to the value stated in the Policy Schedule to rectify and **restore your electronic device(s).** If **we** are unable to repair **your electronic device(s)** then **we** will replace it with a similar make and model up to the value stated in the Policy Schedule.	14
F	Social Engineering	In the event **you** are a victim of a **social engineering attack(s)** and funds have been transferred by **you**, **we** will reimburse **you** up to the value stated in the Policy Schedule for the actual loss **you** have suffered.	15
G	Cyber Security Portal	**You** are provided access to cyber security portal, which provides **you** with a "Personal Cyber Security Score" and tools to help **you** stay safe online.	16
H	Cyber Support Line	**You** are provided access to the Cyber Support Line which will support **you** to identify potential **cyber-attacks** and risks to **your electronic device(s)** and how to deal with these by providing technical advice to prevent **cyber-attacks** from happening and to keep **you** and **your electronic device(s)** safe online.	17

3. Definitions

The following words when used in bold in this document have the meaning given below.

Breach of your privacy means sharing **highly sensitive** private information online with malicious intent via an **electronic device(s).**

Chubb / We / Us / Our means Chubb European Group SE (CEG)

Claim means a request by **you** for any of the entitlements and benefits under sections A to F of this policy.

Cyber-attack means the following malicious or fraudulent acts;

1. Unauthorised access to, and/or use of **your electronic device(s)**;
2. Alterations, corruption, damage, manipulation, misappropriation, deletion of hardware, software and data files on **your electronic device(s);**
3. Transmission or introduction of a computer virus or harmful code including ransomware into **your electronic device(s);**
4. Restriction or inhibition of access targeted at or directed against **your electronic device(s);** and/or
5. Digital account takeover, where the fraudster takes control of **your** electronic accounts which include bank, credit cards, email, social media and other service providers and prevent **you** from accessing them.

Cyber extortion attack means a form of **malware** in which malicious software code prevents **you** from accessing **your electronic device(s)** or encrypts or threatens to encrypt or delete or share personal data including **digital contents**, until a ransom fee is paid.

Cyber harassment means harassing or bullying **you** online by the use of emails, instant messaging, online social platforms and websites likely to cause distress and/or fear of form of violence.

Digital contents mean 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 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 by **payment cards** and **e-money accounts.**

Eligible item(s)/service(s) means any items, services or **digital contents** which are:

1. Purchased solely for personal use; and
2. New and has not been used; and
3. The cost of which has been charged to an eligible card or other eligible payment form under this Policy
4. Not counterfeit or fake goods
5. Not confiscated or illegally declared by any government, customs or public body
6. Not animals or livestock
7. Not classified as real estate
8. Not motor vehicles, motorcycles/scooters, watercraft or aircraft
9. 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.

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**.

Financial loss means monetary loss suffered by **you** in a personal capacity and not related to **your** business interest, if applicable.

Grossly offensive means communication of information electronically (whether verbal or pictorial) which a reasonable person would find disturbing, shocking and/ or beyond the bounds of morality. For the avoidance of doubt, the communication must be more than merely offensive, in bad taste or controversial.

Hacker/Hacked means a **third party** who maliciously targets **you** and gains unauthorised access to **your electronic device(s).**

Highly sensitive means information (whether verbal or pictorial) that (i) would be understood by a reasonable person to fall into a category of information which is inherently private and confidential to **you**, and (ii) **you** have taken reasonable steps to keep confidential. It includes information relating to **your** personal/ intimate relationships, health and/or financial affairs.

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 frequently by others.

Malware means any intrusive software specifically designed to disrupt, damage, or gain unauthorised access to the systems within an **electronic device**.

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 for which they are responsible and/or liable and/or have relevant corporate insurance protection in place.

Payment cards means credit and debit including Chip and PIN, charge, stored value/prepaid and cash card(s), issued by financial institutions, card issuers or retail stores.

Premium means the amount **you** agree to pay **us** in return for the entitlements and benefits of the cover under this policy.

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.

Restore means putting **your electronic device(s)** back to how it was functioning before the **cyber-attack** happened or putting it back to the condition the **electronic device(s)** was in when **you** bought it, which entails reinstalling the operating system and reloading applications that were installed at the time of purchase from the **retailer** or manufacturer.

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 dupe **you** into opening emails, instant messages, text messages and websites from entities or people who **you** trust and/or are known to **you** with the purpose of coercing **you** into transferring funds. Examples of such attacks include phishing, malware phishing, spear phishing, smishing, vishing and pharming.

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**.

You / Your / Policyholder refers to the persons whose name appears on the Policy Schedule and any **family** members where the family product is selected as per the Policy Schedule.

4. Benefits

Section A: Online Shopping Fraud

Cover:

You are covered up to the amount in **your** policy schedule when **you** discover **you** have purchased an **eligible item(s)/service(s)** online from a **third party** for personal use, but the website/trading platform turns out to be fraudulent. The payment for these **eligible item(s)/service(s)** must have been completed using an **electronic transaction(s)** or a bank transfer.

Please note – The intention of this cover is not to indemnify **you** for **electronic transactions** which are completed on genuine websites/ trading platforms, where the legitimate trader:

- 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 Ireland.

In the event **you** are the victim of online shopping fraud:

1. **You** must report it to the Police within 24 hours of **you** discovering the fraud.
2. **You** must contact the cyber claims line on **+353 (0)1 440 1748** as soon as **you** become aware **you** have been a victim of this fraud**.**
3. **You** must demonstrate that **you** have made reasonable attempts to contact the vendor to seek recovery or refund of **your** online purchase.

   You must notify **your payment 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 payment card** issuer/Bank or **e-money account** provider may reimburse **you** for these transactions, but if **your payment 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 payment card** issuer/ Bank or **e-money account** provider then **we** will reimburse **you** for these transactions.

Exclusions under Online Shopping Fraud:

We will not pay any indemnity for*:*

a. Online purchases where cash, crypto currency such as bit coins, voucher or reward point is the form of payment.

b. Unauthorised transactions on **your payment card(s)** or **e-money account** because of this fraud leading to the cloning of **your payment card(s)** or **identity theft**.

Excess applicable to Online Shopping Fraud:
An **excess** will be deducted for each successful **claim.** The **excess** due is shown in the Policy Schedule.

Section B: Cyber Extortion

Cover:

You are covered up to the amount stated in **your** policy schedule in the event **you** suspect **you** have become a victim of **cyber extortion attack**. **You** will be provided with technical support to determine the extent of the attack and provided indemnity to pay the ransom amount subject to the terms and conditions set out below.

If **you** believe **you** are the victim of a **cyber extortion attack**, then:

1. **You** will contact the cyber helpline on **+353 (0)1 440 1748** as soon as **you** notice the **cyber extortion attack** on **your electronic device(s).**

2. The cyber helpline will use its expertise to help **you** identify the nature of the attack. It will determine if **your electronic device(s)** is/are subject to a full lock down or a partial lock down.

3. Depending on the cyber helpline's diagnosis of the attack it will determine the best course of action to take. The cyber helpline **cannot** advise **you** whether **you** should pay the cyber extortion demand.

4. If the only option in **your** view is to pay the extortion amount, then **you** will seek an authorisation code/ confirmation from the cyber helpline. Once this is approved, **you** can make the extortion payment and **we** will reimburse for this amount at the time of payment, up to the maximum amount shown in **your** Policy Schedule.

   Please note – in the event **you** have paid the extortion amount and **your electronic device(s)** has/have not been unlocked by the attacker and/or the attacker is demanding further extortion payments then **you** should seek further advice from **our** cyber helpline. **You** should not attempt to make any further extortion payments.

If **you** choose not to pay the extortion amount, then the cyber helpline will help to **restore your electronic device(s)** including data which is backed up on the cloud or an external storage device. In the event of a loss of data during the **cyber extortion attack** an attempt will be made to recover the data, but no financial benefit will be provided if **we** are unable to recover this data.

Exclusions under Cyber Extortion:

We will not pay any costs for:

1. Cyber extortion payment where an authorisation code/ confirmation has not been obtained from the cyber helpline beforehand;

2. Any **electronic device(s)** which are registered and owned by **your** business, if this is applicable;

3. **Financial loss** of not being able to use the **electronic device(s)** following the **cyber extortion attack** or recover lost data; and

4. Personal data including media contents which is damaged or cannot be restored because of the **cyber extortion attack.**

Excess applicable to Cyber Extortion:
An **excess** will be deducted for each successful **claim**. The **excess** due is shown in the Policy Schedule.

Section C: Identity Theft

Cover:

You are covered up to the amount stated in **your** policy schedule in the event **you** are a victim of **identity theft. You** will be indemnified for legal expense and loss of income.

In the event your identify has been stolen, then:

1. **You** must report the incident of **identity theft** to the Police within 24 hours of **you** discovering the incident. The Police should provide **you** with a reference number which **you** must provide to **us** when making a **claim** under Identity Theft.

2. **We** will pay for legal expense up to the sum insured in **your** policy, which is reasonable to engage with a legal advisor to help **you**:

   a. Stop any further frequent use of **your** identity;

   b. Restore **your** credit rating;

   c. Restore **your e-money**, bank, mortgage or loan account;

   d. Amend or rectify records regarding **your** true name or identity

   e. To defend any suit brought against **you** by a creditor or collection agency or other entity acting on behalf of a creditor for non-payment of good or service or default on a loan;

   f. To remove any civil judgement wrongfully entered against **you**.

3. **We** will pay for personal loss of income up to the amount stated in **your** policy

schedule, which is reasonable due to time taken from **your** work and away from **your** work premises. This includes annual leave taken by **you** (including discretionary days, floating holidays, and paid personal days but excluding sick days) to rectify **your** identity following the **theft** of **your** identity.

Exclusions under Identity Theft:

We will not pay any cost for:

1. Settling fraudulent transaction following the **theft** of **your** identity such as paying back your e-money, bank or building society account or repaying the credit obtained under **your** name;

2. Any loss arising from any business pursuits or the **theft** of a commercial identity;

3. Any loss or liability arising from the use of any motor vehicle bought, leased or hired by fraudulent use of **your** identity, where civil or criminal action is, or has been, taken against **you**;

4. Any loss or liability arising from purchasing/renting any property or real estate using **your** identity, where civil or criminal action is, or has been, taken against **you**;

5. Authorised charges that **you** have disputed based on the quality of goods or services;

6. Any loss of income, costs or expenses in connection with any **claim** not agreed in advance by **us**;

7. Authorised account transactions or trades that **you** had disputed, or are disputing, based on the execution (or non-execution) of electronic transfers, trades or other verbal or written instructions or directions;

8. An incident of **identity theft** for which **you** do not have a Police crime reference number.

Excess applicable to Identity Theft:
An **excess** will be deducted for each successful **claim**. The **excess** due is shown in the Policy Schedule.

Section D: Cyber Bullying

Cover:

In the event **you** are a victim of **cyber harassment** or **breach of your privacy,** subject to **your claim** meeting certain qualifying conditions set out below**, we** will provide **you** with cover to seek professional advice and representation from **your** chosen legal advisers to help **you** remove or suppress the online contents up to the amount stated in **your** policy schedule.
Qualifying conditions to pursue a **claim** for:

1. **cyber harassment:** it must be of a **grossly offensive** nature and the publication or general messaging must have occurred more than 5 times.

2. **breach of your privacy**: the publication online must be malicious and **highly sensitive**.

Please note – if the **claim** does not meet the criteria of this policy and the terms within, it does NOT necessarily mean **you** do not have a valid legal case and **you** should still seek independent legal advice.

If **you** believe **you** are the victim of **cyber harassment** or have suffered a **breach of your privacy**, then:
You must contact **our** Cyber Claims Line on **+353 (0)1 440 1748** who will assess if **you** meet the qualifying conditions to pursue **your claim**.

If **your claim** is accepted and **your** supporting evidence for this **claim** is accepted by **your** chosen legal advisers, then **you** will be entitled to a consultation with **your** chosen legal advisers. They will review the case with **you** and determine **your** objectives to remove or supress the contents of the online **cyber harassment** or **breach of your privacy** or both and provide **you** with recommendations.

If **your** chosen legal advisers in their professional capacity feel that following their consultations and recommendations:

1. **You** have an actionable **claim** in harassment or misuse of private information that is likely to succeed in a civil court; and

2. There is more than 50% chance of achieving the cessation of the harassment and removal of any offending online contents.

Then they will provide **you** with further legal advice and representation up to the sum insured in **your** Policy Schedule.

Exclusions under Cyber Bullying:

We will not pay any costs:

1. if the individual or group of individuals bullying **you** includes relatives and/or immediate **family** members;

2. for legal support to pursue compensation from the harasser unless it is incidental to the legal action to prevent the removal of contents and/or ongoing harassment and is not going to materially reduce the prospects of achieving those objectives. This can be pursued at **your** own expense;

3. for **financial loss** because of not being able to carry out **your** daily tasks like going to work or pursuing other personal interests**;** and/or.

4. if the information has already been placed in the public domain by **you** or is public knowledge.

Excess applicable to Cyber Bullying: An **excess** will be deducted for each successful **claim**. The **excess** due is shown in the Policy Schedule.

Section E: Hacker Damage

Cover:

You are covered up to the amount stated in **your** policy schedule in the event **your electronic device(s)** is/ are hacked following a **cyber-attack**, **we** will provide **you** with technical support through **our** partners to diagnose the extent of the damage to **your electronic device(s)** and indemnify **you** to resolve this**.**

If **your electronic device(s)** is/are **hacked** following a **cyber-attack**:

1. **You** must contact the Cyber Claims Line on **+353 (0)1 440 1748** as soon as **you** suspect a **cyber-attack** on **your electronic device(s).**

2. The Cyber Claims Line will help **you** to determine the best course of action to take to resolve and **restore your electronic device(s)** by:

    a. Using its expertise over the phone or using its online portal to fix the issues and **restore your electronic device(s).**

    b. If the outcome in section **2a** is unsuccessful, then the Cyber Claims Line will put **you** in touch with **our** repair centre, to send in **your electronic device(s)** for assessment and to examine the extent of the damage. Once this assessment is completed, **our** repair centre will either:

        i. Repair and **restore your electronic device(s);** or

        ii. Provide a replacement **electronic device(s)**. **We** will make every effort to replace **your electronic device(s)** with one of the same brand, model, specification and colour, but due to the fast evolution of **electronic device(s)** this cannot be guaranteed, nor can **we** guarantee to replace limited or special edition models.

Please note – This is not 'new for old' cover, and a replacement device may be a refurbished device rather than a brand-new device, depending on availability of similar devices to these that have been subject to a **cyber-attack**.
In the event of a loss of data during the **cyber-attack**

an attempt will be made to recover the data, but no financial benefit will be provided if **we** are unable to recover this data.

This policy will not cover any failure to **your electronic device(s)** that is not a result of a confirmed **cyber-attack**, which will be assessed by the Cyber Support Line and/or repair centre.

Exclusions under Hacker Damage:

We will not pay any costs for:

1. **Financial loss** of not being able to use the **electronic device(s)** following the **cyber-attack** or recover lost data or whilst the **electronic device(s)** is/are being repaired;
2. Any **electronic device(s)** which is/are registered and owned by **your** business, if this is applicable;
3. **Accidental damage** to the hardware or software;
4. **Malicious damage** to the hardware or software which was not directly caused by the **cyber-attack**;
5. Wear and tear or gradual deterioration of performance of **your electronic device(s);**
6. Any damage to **your electronic device(s)** as a result of mechanical breakdown;
7. Any **Jail broken electronic device(s)**;
8. Any data that is hacked from an external hard drive or from the cloud or equivalent online; storage/backup facility which leads to **your** Identity being stolen or used to commit acts of fraud;
9. Any loss of data which is has not been backed up either on
    a. An external hard-drive which is independent from the impacted device or;
    b. On the cloud or equivalent online storage/backup facility and;
10. **Digital contents** which cannot be recovered.

Excess applicable to Hacker Damage: An **excess** will be applicable if the **electronic device(s)** must be repaired or replaced as per condition 2(b) under "Cover". The **excess** due is shown in the Policy Schedule.

Section F: Social Engineering

Cover:

You are covered up to the amount stated in **your** policy schedule in the event **you** are a victim of a **social engineering attack** requesting **you** to transfer funds from **your** personal account to the account of a **third party** and **you** transfer funds as a direct result of such request, **we** will reimburse **you** for funds **you** have transferred up to the sum insured in your Policy Schedule.

In the event **you** are a victim of a **social engineering attack:**

1. **You** must report it to the Police within 24 hours of **you** discovering the fraud.

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 contact the cyber claims line on **+353 (0)1 440 1748**, as soon as **you** become aware **you** have been a victim of a **social engineering attack;** and

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;** and

    b. that the person was entitled to receive payment.

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, then **we** will reimburse **you** for these transactions.

Exclusions under Social Engineering:

We will not pay any costs for:

1. any transfer from a business account; or

2. any advance fee fraud where **you** are promised a significant amount of money, in return for an upfront payment including payment by **electronic transaction(s)**.

Excess applicable to Social Engineering:
An **excess** will be deducted for each successful **claim**. The **excess** due is shown in the Policy Schedule.

Section G: Cyber Security Portal

Cover:

During the period of **your** policy, **you** are provided with access to cyber security portal, which provides **you** with a "Personal Cyber Security Score" and reports to help **you** stay safe online. The software 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. Depending on the type of cover you have selected (individual or family cover), **you** will be provided with:

1. Individual cover:
    a. Monitoring up to 2 personal email addresses
    b. Device vulnerability protection for 3 **electronic device(s)**
    c. Router vulnerability protection
    d. Scam prevention training and alerts

2. Family cover:
    a. Monitoring up to 10 personal email addresses of **yours**
    b. Device vulnerability protection for 10 **electronic device(s)**
    c. Router vulnerability protection
    d. Scam prevention training and alerts

Section H: Cyber Support Line

Cover:

You will also be able to contact the Cyber Support Line on **+353 (0)1 440 1748** who can help **you** to: improve the security of **your electronic device(s)**; stop viruses infecting **your electronic device(s)**; and help **you** to identify when **your** personal information has been stolen so **you** can take appropriate action.

5. Terms and Conditions applicable to all sections

General Exclusions

This policy does not provide cover for losses under any sections of these Terms and Conditions which are recoverable from any other sources such as, but not limited to **your** Bank, **your payment card(s)** provider, third party payment platforms etc, or arising from:

1. Any incident prior to the start date of **your** insurance policy or after the cancellation;
2. The first amount of every successful **claim** (the **excess**), wherever applicable;
3. 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**; and
4. 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.
5. A potential **mass cyber-attack**.

General Conditions

1. **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.
2. **You** must take reasonable steps to avoid future loss.
3. For each of the benefits, regardless of the number of **claims** made individually or in aggregate, **we** will pay up to the maximum amount per occurrence as shown in the Policy Schedule.
4. **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.
5. **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.
6. **You** must be a resident of the Republic of Ireland at the time of application for this insurance and remain a resident of that country during the term of this policy. If **you** are planning to move to another country, **you** must contact **us** on **1800 320 320** to see if this policy can remain in force.

6. to make a claim

When making a **claim you** must:

1. the Cyber Claims Line on **+353 (0)1 440 1748** or our online claims portal at **https://intake.sedgwick.com/u/ChubbIreland/Chubb**
2. **your** Policy Number (as shown on **your** Policy Schedule).
3. all **your** original invoices, receipts, reports including crime reference number where applicable and any other documentation necessary to support **your claim**; and
4. **proof of purchase** for items being claimed. 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** that may be payable.

Please first read the relevant Section of the specific benefit and general terms and conditions to determine what is covered, noting particularly conditions and exclusions and/or requests for specific data relating to **your claim**.

7. 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 in accordance with **our** cancellation rights set out in Section 9 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.

8. Changing your policy

If **you** want to change **your** policy or if **your** insurance needs or any of the information **you** have given **us** changes, **you** must telephone **us** on **1800 320 320** or email **us** on **Anpostinsurance.cyber@Chubb.com**

We reserve the right to make changes, add to the policy terms under this policy for valid reasons, for example, legal, regulatory or taxation reasons or increases in the cost of fulfilling claims. If this happens, **we** will write to **you** with details of the changes at least 60 days before **we** make them.

9. Cancelling your policy

Your rights to cancel this policy:

1. **You** may cancel this policy by either calling **1800 320 320** or emailing **us** on **Anpostinsurance.cyber@Chubb.com**

    a. If, for any reason, **you** are not satisfied with **your** policy, **you** have a statutory right to cancel it within 14 working days of (i) receiving all of **your** policy documents or (ii) the start of the period of cover, whichever is later. If **you** cancel the policy within the 14 working day period, **you** will receive a full refund providing that **you** have not already made a **claim.**

    b. If **you** wish to cancel **your** policy after the initial 14 working day statutory period, **your** cover will expire at the end of the period **you** have paid for. No refund of **premium** will be provided.

Our right to cancel this policy:

1. **We** may cancel this policy by giving **you** a minimum of 30 days' written notice. If **we** do so, **we** will refund any **premium you** have paid that relates to the period after the date of cancellation.

2. **We** will only cancel **your** policy for a valid reason for example:

    a. **You** fail to pay **your** monthly **premium** when due;
    b. **You** commit an act of fraud or willfully seek to mislead **us** in anyway.
    c. A change in regulatory, tax or legal status for **you**, **us** or the policy.

10. Other taxes and costs

We are required to notify **you** that other taxes or costs may exist which are not imposed or charged by **us**.

11. 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 Republic of Ireland and the Irish Courts alone will have jurisdiction in any dispute. All communication in connection with this Policy will be in English.

12. Rights of third parties

Only **you** and **us** can enforce the terms of this Policy. No other party may benefit from this contract as of right. This Policy may be varied or cancelled without the consent of any third party.

13. Assignment

This policy may not be assigned by

you, and **we** will not be bound to accept or be affected by any notice or any trust, charge, purported assignment or other dealing with or relating to this policy.

14. Sanctions

Chubb shall not be deemed to provide cover and **Chubb** shall not 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 **Chubb**, to any sanction, prohibition or restriction implemented pursuant to resolutions of the United Nations or the trade and economic sanctions, laws or regulations of the European Union, United Kingdom, Ireland or United States of America.

15. Data protection statement

We use personal information which **you** supply to **us** in order to write and administer this Policy, including any **claims** arising from it.

This information will include basic contact details such as **your** name, address, and policy number, but may also include more detailed information about **you** (for example, **your** age, health, details of assets, **claims** history) where this is relevant to the risk **we** are insuring, services **we** are providing or to a **claim you** are reporting.

We are part of a global group, and **your** personal information may be shared with **our** group companies in other countries as required to provide coverage under **your** policy or to store **your** information. **We** also use a number of trusted service providers, who will also have access to **your** personal information subject to **our** instructions and control.
You have a number of rights in relation to **your** personal information, including rights of access and, in certain circumstances, erasure.

This section represents a condensed explanation of how **we** use **your** personal information. For more information, **we** strongly recommend **you** read **our** user-friendly Master Privacy Policy, available here: https://www.chubb.com/ie-en/footer/ privacy-policy.html
You can ask **us** for a paper copy of the Privacy Policy at any time, by contacting **us** at: dataprotectionoffice.europe@chubb.com.

16. Complaints procedures

We are committed 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** at the address below, quoting the policy details, so **we** can deal with the complaint as soon as possible:

The Customer Relations Manager
Chubb
5 George's Dock
International Financial Services Centre
Dublin 1
T 01 440 1700

You can approach the Financial Services and Pension Ombudsman for assistance if there is dissatisfaction with **our** final response. Their contact details are given below. A leaflet explaining the procedure is available on request.

Financial Services and Pensions Ombudsman
3rd Floor
Lincoln House
Lincoln Place
Dublin 2
D02 VH29
T (01) 567 7000
E info@fspo.ie
W www.fspo.ie

The existence of these complaint procedures does not reduce an Insured Person's Statutory Rights relating to this Policy. For further information about Statutory Rights, an Insured Person should contact the Competition and Consumer Protection Commission.

17. European online dispute resolution platform

If **you** arranged **your** policy with **us** online or through other electronic means and have been unable to contact **us** either directly or through the Financial Services and Pensions Ombudsman, **you** may wish to register **your** complaint through the European Online Dispute Resolution platform: http://ec.europa.eu/consumers/odr/. **Your** complaint will then be re-directed to the Financial Services and Pensions Ombudsman and to **us** to resolve. There may be a short delay before **we** receive it.

18. Our regulators

Chubb European Group SE trading as Chubb, Chubb Bermuda International and Combined Insurance, is authorised by the Autorité de contrôle prudentiel et de résolution (ACPR) in France and is regulated by the Central Bank of Ireland for conduct of business rules.
Registered in Ireland No. 904967 at 5 George's Dock, Dublin 1.

Chubb European Group SE (CEG) is an undertaking governed by the provisions of the French insurance code with registration number 450 327 374 RCS Nanterre. Registered office : La Tour Carpe Diem,31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, France. CEG has fully paid share capital of €896,176,662.

One Direct (Ireland) Limited, trading as An Post Insurance, is regulated by the Central Bank of Ireland. One Direct (Ireland) Limited is a wholly owned subsidiary of An Post. Registered in Ireland Number 452399. Registered Office: GPO, O'Connell St., Dublin 1. D01 F5P2

Personal Cyber Insurance is arranged, administered and underwritten by Chubb European Group SE.

Chubb European Group SE trading as Chubb, Chubb Bermuda International and Combined Insurance, is authorised by the Autorité de contrôle prudentiel et de résolution(ACPR) in France and is regulated by the Central Bank of Ireland for conduct of business rules. Registered in Ireland No. 904967 at 5 George's Dock, Dublin 1. Chubb European Group SE is an undertaking governed by the provisions of the French insurance code with registration number 450 327 374 RCS Nanterre and the following registered oice: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, France. Chubb European Group SE has fully paid share capital of €896,176,662.

Chubb European Group SE is a subsidiary of a US parent and Chubb Limited (a NYSE listed company) and part of the Chubb Group of companies. Consequently Chubb European Group SE is subject to certain US laws and regulations in addition to EU, UN and national sanctions restrictions which may prohibit it from providing cover or paying claims to certain individuals or entities, and from insuring certain types of activities in or connected with certain countries and territories such as, but not limited to, Iran, Syria, North Korea, North Sudan, Cuba and Crimea.

an post insurance