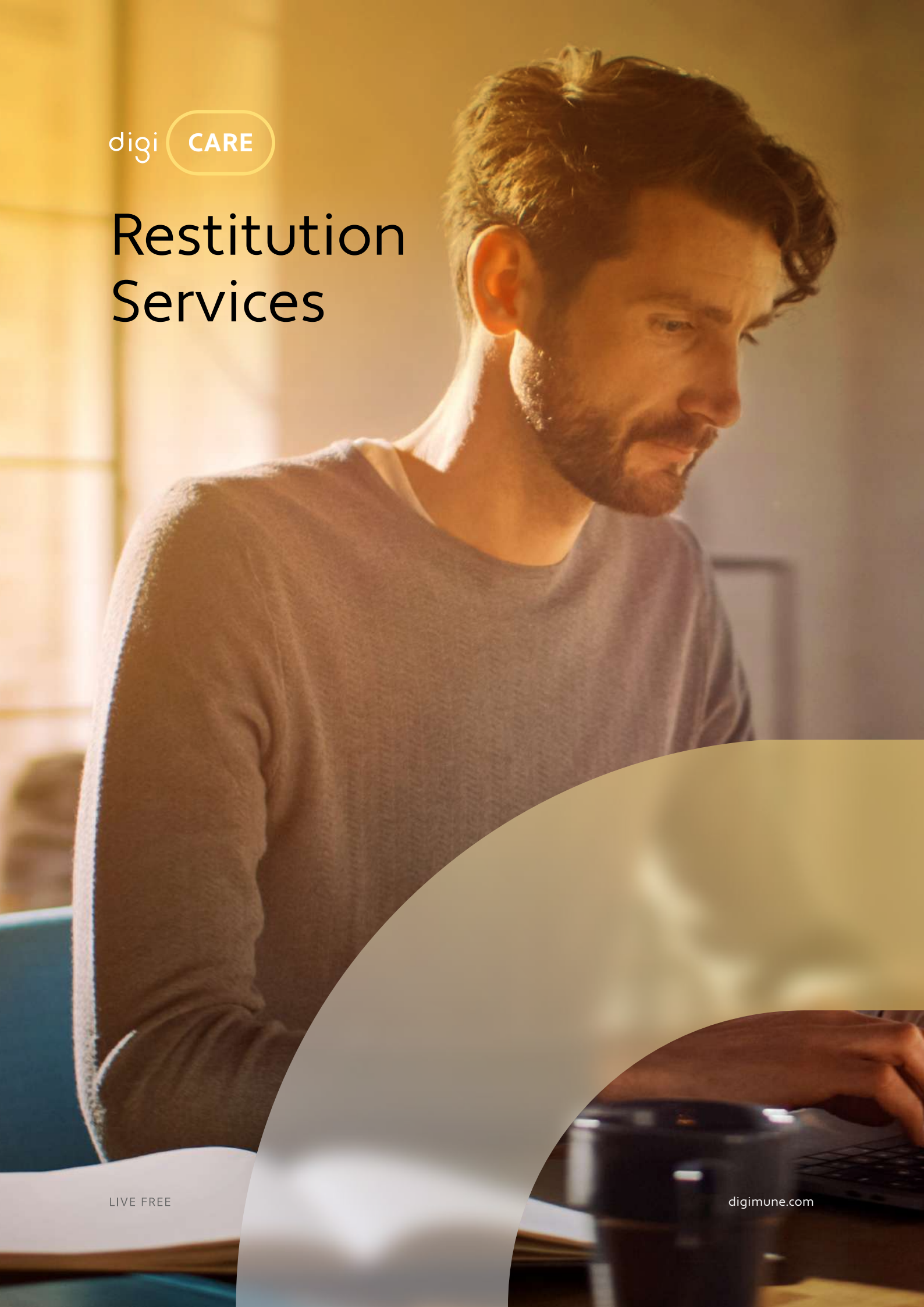
digi CARE

Restitution Services



Restitution Services

1. Definitions

"Legal Costs" means the costs we will pay to qualified legal experts of our choosing to provide you with confidential legal advice and/or representation regarding assessing the legal remedies and steps you may take in response to covered events. It does not include legal advice about this policy.

"Covered Events" means the events where we will take the necessary legal action to protect and secure your legal rights. Your infringed rights that we will protect must relate to the fraudulent use of your identity following an incident relating to identity theft, cyberbullying, cyber stalking or cyber harrassment. In such cases, the following action/s will be taken:

a) Defending you in civil proceedings being entered against you where you are not aware of the civil proceedings; or
b) Rescinding a judgment entered against you where you are not aware of it; or
c) Assisting to seek relief for a negative consumer credit report in your name; or
d) Assisting to seek relief for the unauthorised establishment of credit in your name; or
f) Arranging to obtain an intervention (restraining) order; or
g) Instituting legal action for reputational damages as a result of cyber harassment and harmful publication; or
h) Mitigating a cyberbullying/cyber-stalking incident; or
i) Recovering financial losses, namely the difference between your total losses minus insurance/financial institution payout/recovery. In this instance, the prospects of success must be at least 51% in order for us to pursue the perpetrator. If the funds are recovered and paid into your own account, you must, as soon as possible, advise us and repay the funds recovered into our account. The jurisdiction to pursue is global.

"Panel of Practitioners" means our team of knowledgeable, experienced and registered experts who will act on your behalf.

"Cyberbullying" means tormenting, harassing, humiliating, embarrassing or otherwise targeting a child, preteen or teen (up to and including 19 years of age) by another person, as evidenced by electronic communication. For example, using the internet or a mobile phone to hurt or call names, excluding or ignoring someone, tricking or humiliating someone through fake accounts or sharing a photo or video that will make the victim feel bad.

Threatening to share an intimate image without someone's consent (a naked selfie) is known as image-based abuse. These abusive actions may lead to self-harm, suicidal thoughts, emotional volatility, refusal or inability to attend school or participate in usual organised extracurricular activities, or withdrawal or resignation from these.

"Cyber Stalking" means any activity relating to sending, transmitting or publishing offensive material via phone or web technology. It also includes any other incident that could be reasonably expected to arouse the other person's apprehension or fear by the unwanted and persistent tracking of their whereabouts, monitoring communications or activities – or the ongoing receipt of targeted emails, texts, messages, phone or video calls or any other material with threatening effect.

"Cyber Harassment" means a specific threat by a third party to publish personal information (obtained as a result of a cyber event) about you on the internet, which has the potential to damage your reputation.

2. Process Of Assistance

2.1 **Telephonic Legal Advice** on how to file a complaint with a utility provider, police department or law enforcement to resolve infringed rights.
2.2 **Dispute Resolution (Mediation)** via virtual meetings with victim/parent/childminder.
2.3 **Psychological Assistance** via virtual meeting with the victim/parent/childminder.
2.4 **Appoint Panel Experts** to obtain information and evidence in order to build the case.
2.5 **Intervention Order** (Prevention of Abuse, Act 2009) assistance when the victim has been cyberbullied, cyber stalked or cyber harassed.

2.6 **Restitution Court Action** against the perpetrator to claim damages, compensation and financial losses.
2.7 **Victim Defence** in the unlikely event that the victim is arrested and detained for illegal acts committed by the perpetrator as a result of identity theft.
2.8 **Rescission of Judgments** attendance to clear the victim's credit record.
2.9 **Bail Money** of USD 1,000 (or local currency equivalent) if the victim is unlawfully arrested and detained for an illegal act committed by the perpetrator.
2.10 **Arranging Bail** with the prosecuting authorities.
2.11 **Bail Hearing** representation.

3. Claims Process

3.1 **Identity Theft Breach** – this process starts by receiving data and information from the insurer, technical stack team, authorities, utility providers and victim to:
   a) Assess the breach and track data sources and origin.
   b) Scrutinise data and information to hunt down and track the perpetrator and to establish the perpetrator's address of operation and modus operandi;
   c) Identify the impersonating data and obtain evidence to build the case and finalise reports;
   d) Engage with credit bureaus on the status of the victim's credit profile and query any additional adverse reports;
   e) Institute legal action on behalf of the victim against the perpetrator/utility provider to sue for financial losses, pain, suffering and reputational damages;
   f) Defend the victim in a criminal bail hearing when wrongfully accused of fraud charges and provide bail money;
   g) Defend the victim in a civil court when wrongfully accused of owing debt as a result of identity theft; and
   h) Rescind any wrongful judgment taken against the victim due to identity theft.

3.2 **Cyberbullying/Cyber Stalking/Cyber Harassment** – the process starts by receiving data and information on the rude comments or posts from the victim, parent, teacher and cybercrime team to:
   a) Analyse and assess the screenshots and recordings of the unsolicited message, threatening text, call, photo or video uploads on the internet without the victim's permission;

b) Assess the feelings of hurt, sadness or anger, which may lead to feelings of depression, anxiety or self-esteem issues and put the victim in contact with a psychologist or counsellor;
c) Advise on ways to eliminate the ongoing action by blocking the perpetrator on social platforms, changing a phone number and/or email address and/or privacy settings and/or refrain from making any further comments and/or provide less personal information;
d) Obtain information about the perpetrator;
e) Involve the police and law enforcement authorities to obtain a protection/ intervention order.

4. How To Claim

4.1 Contact Digimune's DigiCare Support Team to lodge an intent to claim as soon as possible after the incident, but within **30 (thirty) days** of the discovery. The sooner the victim notifies Digimune's DigiCare Support Team, the sooner there can be assistance.
4.2 Digimune's DigiCare Support Team will need to verify that the victim's product is active, valid, and up to date with payments.
4.3 In order to process the claim, Digimune's DigiCare Support Team may request documentation from the victim to verify the claim. Do note – any cost associated with obtaining the required documentation will not be covered by Digimune.
4.4 Documentation to be provided by the victim may include, but is not limited to, the police report and case number, name and contact details of the investigating officer, name and details of the cyberbully/cyber stalker/cyber harasser, and (if available) any photographs, videos, screenshots, messages and recordings etc.
4.5 Inform Digimune's DigiCare Support Team when you become aware of any possible prosecution, legal proceedings or claim that could be lodged against you as a result of the cybercrime incident.
4.6 We will only process claims for an incident, or event that occurred after the date that You enrolled under the Digimune Digital Protection Programme, but before the expiration date of that programme.
4.7 Legal and practitioner fees paid on your behalf will be limited to USD 5,000 (or local currency equivalent) during a 12-month period.

For any queries relating to this document,
please contact us via the details below.

SOUTH AFRICA
Workshop 17
32 Kloof Street
Cape Town
8001

t: +27 (0) 11 463 1309

UNITED KINGDOM
C/O Haggards
Heathmans House
19 Heathmans Road
London
SW6 4TJ

general enquiries: connect@digimune.com
support: support@digimune.com
claims: claims@digimune.com