digi CARE

Restitution Services

1. Introduction

This product provides Restitution Assistance Services in the unlikely event of a cyber incident, specifically in circumstances where the Digimune tech stack has failed and the client has been exposed to a cyber incident related to Identity Theft, Cyberbullying, Cyberstalking, Cyber harassment, or Image-based abuse.

2. Definitions

- **Assistance Services** means:
  - Defending you in civil proceedings being entered against you where you are not aware of the civil proceedings; or
  - Rescinding a judgment entered against you where you are not aware of it; or
  - Assisting to seek relief for a negative consumer credit report in your name; or
  - Assisting to seek relief for the unauthorised establishment of credit in your name; or
  - Arranging to obtain an intervention (restraining) order; or
  - Instituting legal action for reputational damages as a result of cyber harassment and a harmful publication; or
  - Mitigating a cyberbullying/cyberstalking incident; or
  - Recovering financial losses to specified limits 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.
- **Cyberbullying** refers to 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, this may include using the internet or a mobile phone to hurt someone or call them names, excluding or ignoring someone, tricking or humiliating someone through fake accounts, or sharing a photo or video intended to make the victim feel bad.
- **Image-Based Abuse** involves threatening to share an intimate image without someone's consent (such as a naked selfie). These abusive actions can lead to self-harm, suicidal thoughts, emotional volatility, refusal or inability to attend school or participate in usual organized extracurricular activities, or withdrawal from these activities.

- **Cyberstalking** encompasses any activity related to sending, transmitting, or publishing offensive material via phone or web technology. It also includes any other incidents that could reasonably be expected to instil apprehension or fear in another person due to the unwanted and persistent tracking of their whereabouts, monitoring their communications or activities, or the ongoing receipt of targeted emails, texts, messages, phone or video calls, or any other threatening material.

- **Cyber harassment** refers to 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.

- **Legal Costs** refer to the expenses we will cover for qualified legal experts of our choosing to provide you with confidential legal advice and/or representation regarding the assessment of legal remedies and the steps you may take in response to covered events. It does not include legal advice concerning this policy.

- **Panel Experts** refers to our team of knowledgeable, experienced, and registered experts who will act on your behalf.

- **Territory** means worldwide.

3. Process Of Assistance

We will assist you in identifying the most appropriate legal path by discussing different options, providing clarity on the circumstances, gathering relevant evidence, submitting and lodging disputes with key stakeholders in the cyber industry, liaising with cyber investigators and authorities, keeping you informed on the progress, and working to mitigate and mediate a favourable outcome. The different methods to be utilised consists of:

- **Telephonic advice and assistance to complete forms** and on how to file a complaint with a utility provider, police department, or law enforcement to address infringed rights.

- **Mediation** through virtual meetings with the victim, parent, or childminder.

- **Psychological assistance** via virtual meetings with the victim, parent, or childminder.

- **Appointment of panel experts** to gather information and evidence necessary to build the case.

- **Intervention and protection order assistance** for victims of cyberbullying, cyberstalking, or cyber harassment.

- **Restitution court action** against the perpetrator to claim damages, compensation, and financial losses.

- **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.

- **Rescission of judgments** to help clear the victim's credit record.

- **Bail money** of USD 1,000 (or the local currency equivalent) if the victim is unlawfully arrested and detained for an illegal act committed by the perpetrator.

- **Arranging bail** with the prosecuting authorities.
- **Representation at bail hearings**.

4. Claims Process

- **Identity Theft Breach** – This process begins by gathering data and information from the insurer, technical stack team, authorities, utility providers, and the victim to:

  - Assess the breach and track data sources and origins.
  - Scrutinize the data and information to identify and track the perpetrator, establishing the perpetrator's operational address and modus operandi.
  - Identify the impersonating data and obtain evidence to build the case and finalize reports.
  - Engage with credit bureaus regarding the status of the victim's credit profile and query any additional adverse reports.
  - Institute legal action on behalf of the victim against the perpetrator or utility provider to seek compensation for financial losses, pain, suffering, and reputational damages.
  - Defend the victim in a criminal bail hearing if wrongfully accused of fraud and provide bail money as needed.
  - Defend the victim in civil court if wrongfully accused of owing debt as a result of identity theft.
  - Rescind any wrongful judgments taken against the victim due to identity theft.

- **Cyberbullying/Cyberstalking/Cyber-harassment/Image Based Abuse** – This process begins by collecting data and information regarding rude comments or posts from the victim, parent, teacher, by the cybercrime team to:

  - Analyse and assess the screenshots and recordings of unsolicited messages, threatening texts, calls, and photo or video uploads on the internet made without the victim's permission.
  - Evaluate the emotional impact, such as feelings of hurt, sadness, or anger, which may lead to depression, anxiety, or self-esteem issues, and connect the victim with a psychologist or counsellor.
  - Advise on ways to eliminate ongoing harassment by blocking the perpetrator on social platforms, changing phone numbers and/or email addresses, updating privacy settings, refraining from making further comments, and/or providing less personal information.
  - Appoint investigators to obtain information about the perpetrator.
  - Involve the police and law enforcement authorities to secure a protection or intervention order.

5. How To Claim

- Contact the Digimune Support Team to lodge an intent to claim as soon as possible after the incident, but within 30 days of its discovery. The sooner the victim notifies the Digimune Support Team, the sooner assistance can be provided.
- The Digimune Support Team will need to verify that the victim's product is active, valid, and up to date with payments.
- To process the claim, the Digimune Support Team may request documentation from the victim to verify the claim. Please note that any costs associated with obtaining the required documentation will not be covered by Digimune.
- Documentation that the victim may need to provide includes, but is not limited to, the police report and case number, the name and contact details of the investigating officer, the name and details of the cyberbully, cyberstalker, or cyberharasser or image base abuser, and any available photographs, videos, screenshots, messages, and recordings.
- Inform the Digimune Support Team as soon as you become aware of any possible prosecution, legal proceedings, or claims that could be lodged against you as a result of the cybercrime incident.
- We will only process claims for incidents or events that occurred after you enrolled in the Digimune Digital Protection Programme and before the expiration date of that programme.
- Legal and practitioner fees paid on your behalf will be limited to USD 5,000 (or the local currency equivalent) during a 12-month period.

6. Disclaimer

The information provided above is for informational purposes only and should not be regarded as financial advice. For any financial advice related to this product, please contact Community Legal Clinic (Pty) Ltd | Authorised Financial Services Provider | FSP No. 39887. This product is part of the Digimune warranty and may not be sold separately.