

Personal Cyber Protection for only \$175



We are excited to announce that "Cyberman365" from Node International in partnership with Flood Risk Solutions is available to you and offers up to \$1 million in ID Theft Insurance and Restoration Support. In the unfortunate event of an Identity Theft incident Node International's U.S.-based Fraud Resolution Agent will provide step-by-step assistance to investigate and restore your identity in the event of a claim. With a Limited Power of Attorney, Node International can manage the recovery process on your behalf and provide extra protection at no additional cost after a claim.

Additionally, as a standalone, subscription-based service, Cyberman365 React offers far more robust coverage than what is otherwise available in the marketplace. For only \$175 per year for the family, this policy provides one of the most comprehensive and cost effective programs available in the marketplace.

To purchase the policy, please follow the link at <u>www.floodsol/cyberman365</u>. If you have any questions, please do not hesitate to contact me.

Brendan Moeller, CPCU Managing Director <u>bm@floosol.com</u> (813) 336-8826





Coverage Overview

Claim upto \$1 million

Your aggregate limit is \$1,000,000 per policy period

ID Restoration Support

A Fraud Resolution Agent will deliver step-by-step support to restore your identity. Our Limited Power of Attorney option allows our agents to manage recovery on your behalf.

ID Theft Insurance

You are covered up to \$1 million for certain eligible expenses associated with ID theft. including lost wages, legal fees and electronic fund transfers.

CyberAgent Dark Web Monitoring

We scan the dark web, known for illegally buying and selling personal data and alert you if your identity may be at risk. We will assist you in securing any breached data.

Credit Monitoring

We will alert you to any critical changes by constantly monitoring your credit(s) reports. You will also receive a credit report upon enrollment.

Bank Account Takeover

We alert you if your identity is used to open new bank accounts or if unauthorized changes are made to existing accounts. We will then help you resolve the problem.

Cyber Bullying

Coverage for necessary and reasonable cyber bullying expenses i.e. counselling, replacement wages, educational relocation expenses and legal services.

Internet of Things Compromise

Coverage for necessary and reasonable costs for data recovery and system restoration following a "cyber-attack" (defined as unauthorised access or use and/or a malware attack).

Key elements of their coverage offerings include:

ID Theft

- Cyber Bullying
- CyberAgent Dark Web Monitoring
- Credit Monitoring
- Online Fraud
- Child Social Network Monitoring

Zero Deductible

You don't need to pay anything out of pocket before your coverage kicks in

Change of Address

If your mail is redirected through the U.S. Postal Service, you will receive an alert. This is an easy way for fraudsters to collect your data and abuse your identity.

Online Fraud

Coverage for necessary and reasonable fraud costs (including direct financial loss), so long as it has been reported in writing to the Police.

Child Social Network Monitoring

Scans your child's social media accounts and informs you if privacy or reputational risks are spotted on their profile. Includes Twitter, Facebook, Instagram and LinkedIn

Social Security Number Trace

If a new name or alias is added to your SSN we will alert you, we also generate a report of all the names and aliases already associated with your SSN.

Child Internet Surveillance Report

We scan the dark web, known for illegally buying and selling personal data, and alert you if your child's identity may be at risk. We will assist you in securing any breached data.

Cyber Extortion

Coverage for the costs of an expert to help with a cyber extortion event, as well as reasonable costs to respond to an extortion threat.

Social Media Monitoring

Scans your social media accounts and informs you if privacy or reputational risks are spotted on your profile.





F LI

Malware & Viruses

Criminals use tactics to infiltrate your devices and may steal information and hold your device and files for ransom until you pay a fee.



Change of Address

With just a name and address someone can divert your mail. They can then collect additional information about you such as credit card information or your Social Security Number.

How ID Theft Can Happen



Data Breaches

Unfortunately companies often fall victim to data breaches where customers' personal information is exposed. This means criminals can get hold of your data.



Wallet Theft

If someone gets hold of your wallet, think about how much information they would have on you, SSN, name, age, bank accounts, health insurance details and more.



Mail Theft

If you have an unlocked mailbox, identity thieves can easily steal your mail containing your personal information. This also applies to your garbage so make sure you shred any personal data.



Oversharing on Social Media

Always be aware of what you are sharing, if strangers can predict your movements it's easy for them to steal your identity or belongings.



Claim EXAMPLES

ID Theft

Discovering your personal info stolen, leading to fraudulent credit cards, loans, and government benefits in your name, damages your credit score. Struggling to clear your name, you face endless calls with creditors, battling to prove your innocence. The emotional toll is heavy, leaving you violated and powerless.

Phishing Scams

You get an email resembling your bank's official communication, asking urgently to verify your account details via a link. Despite your caution, you're caught off guard and click, entering your login info. Soon, you receive another email confirming changes to your account, and your balance is emptied. Panic ensues as you realize you've fallen for a phishing scam, scrambling to freeze your accounts and contact your bank to prevent further damage.

Ransomware Attack

Imagine finding all your files encrypted one morning—a ransomware attack demands a hefty Bitcoin payment for access. As a freelancer, losing these files threatens your livelihood. Desperate to retrieve them, you contemplate paying the ransom, but fear dealing with cybercriminals and uncertain if they'll decrypt your files. With looming deadlines and demanding clients, stress mounts in an already dire situation.

Online Fraud

You've saved for months to buy a designer handbag from an online store you found on social media. Despite its professional appearance and reasonable prices, your order never arrives. Frantic emails to the company go unanswered, and you realize too late that it's a scam. Losing money, you feel foolish and vow to be more cautious with online retailers, even if it means passing up good deals.

Cyber Bullying

Your teenage daughter confides in you about cyberbullying, receiving cruel messages from classmates on social media, hurting her confidence and well-being. Despite efforts with school administrators, the cyberbullying persists, leaving you feeling helpless and frustrated with inadequate measures against online harassment.

Social Engineering Attack

You get a call from a supposed tech company rep, claiming your computer has a virus. They instruct you to download remote access software to fix it. But instead, it gives them unrestricted access, letting them monitor, steal sensitive info, and launch cyber attacks using your device. Feeling violated, you're now wary of unsolicited communication via phone, email, or text.

Data Breaches

Your healthcare provider notifies you of a breach, revealing your personal health info, including medical history and insurance details, might be compromised. Anxiety grips you, fearing the consequences for your privacy and financial security. You ponder how the breach happened and what measures you can take to safeguard against identity theft and fraud.

Unauthorized Access

You notice unusual activity on your social media—posts and messages you didn't make. Investigation reveals your accounts are hacked, spreading spam and phishing links. Feeling violated and embarrassed, you worry about reputation damage. After regaining control with new passwords and two-factor authentication, you wonder how they accessed your accounts and how to prevent future breaches.

Online Extortion

You get an email demanding money in exchange for not releasing intimate photos and videos of you. Shocked, you realize someone has compromising material without your consent, using it to blackmail you. Fearful of public exposure, you debate paying to protect your privacy or refusing the demands. Feeling ashamed and vulnerable, you dread the possibility of your private moments being exposed against your will.

Online Scams

You spot an appealing online ad for a work-from-home gig, pledging big earnings with little effort. Hoping to boost income, you sign up, investing heavily in training and fees. But as you explore further, you find the returns unrealistic and the focus on recruiting, not genuine work. Realizing it's a pyramid scheme, you're frustrated and vow to be cautious with online opportunities.