



TransUnion Dark Web Monitoring

Keep your customers' data in the light



Increase cyber awareness by alerting customers to dark web exposure



Mitigate fraud-related risks with real-time monitoring



Strengthen customer relationships through meaningful touchpoints

Proactively monitor the dark web and mitigate data breach concerns

The rise of deception cases in Hong Kong, largely due to personal data leaks on the dark web, has made cybersecurity a top concern for consumers.

TransUnion Dark Web Monitoring offers a vigilant, 24/7 safeguard against these threats, enabling businesses to empower their customers.

Our service not only proactively scans for compromised data but also provides actionable steps for damage control, enhancing your brand's trustworthiness and customer retention.

Key insights from our consumer survey on identity fraud and protection (Sept.2023)

1. High exposure to fraud



74% of consumers have been targeted by online, email, phone, or text fraud.

2. Victimization rates



13% actually became victims of fraud.

3. Financial impact



87% of victims suffered monetary loss.



33% lost more than HK \$50,000.

4. Dark web concerns



60% are concerned about dark web scams.

5. Identity theft worries



56% are concerned about identity theft or fraud.

6. Lack of monitoring



88% are not using dark web monitoring tools.

Source: Identity Fraud & Protection Survey, TransUnion HK, Sep 2023

The alarming rise of cyber fraud*



52.1% Year-over-Year increase in deception cases



\$2.69B Lost to online deception cases



75% Online fraud cases



192 Cases successfully stopped

*Source: HKSAR – Law and order situation in the first half of 2023

Features

Dark Web Monitoring equips businesses with a robust set of features that enhance cybersecurity and add significant value to customer relationships — an extra layer of protection for your customers in today's digital landscape.

24/7 worldwide cybersecurity guard

Continuous monitoring of hard-to-find dark web sites minimises risk exposure and offers your customers peace of mind.

Covering almost all important personal data

From names and IDs to bank accounts and gamertags, extended data coverage enhances customer trust by safeguarding the most critical personal information.

Types of data monitored by TransUnion Dark Web Monitoring

All data monitored adheres to TransUnion's stringent privacy standards



Name



Passport number



Email address



Bank account number



Username



HKID number



Date of birth



Telephone number



Credit card number



Gamertag

Additional resource: Credit Alert Service for enhanced financial security

Complementing Dark Web Monitoring, our Credit Alert Service notifies your customers of key changes to their credit accounts, further solidifying your position as a committed security partner.

Key changes monitored include:

- New inquiries made to your customer's credit report
- New credit accounts opened under your customer's name
- Changes in your customer's registered address
- Updates to your customer's phone number

LEARN MORE:

Contact your **TransUnion representative** to unlock the full potential of cybersecurity for your business with **Dark Web Monitoring** and **Credit Alert Service**.