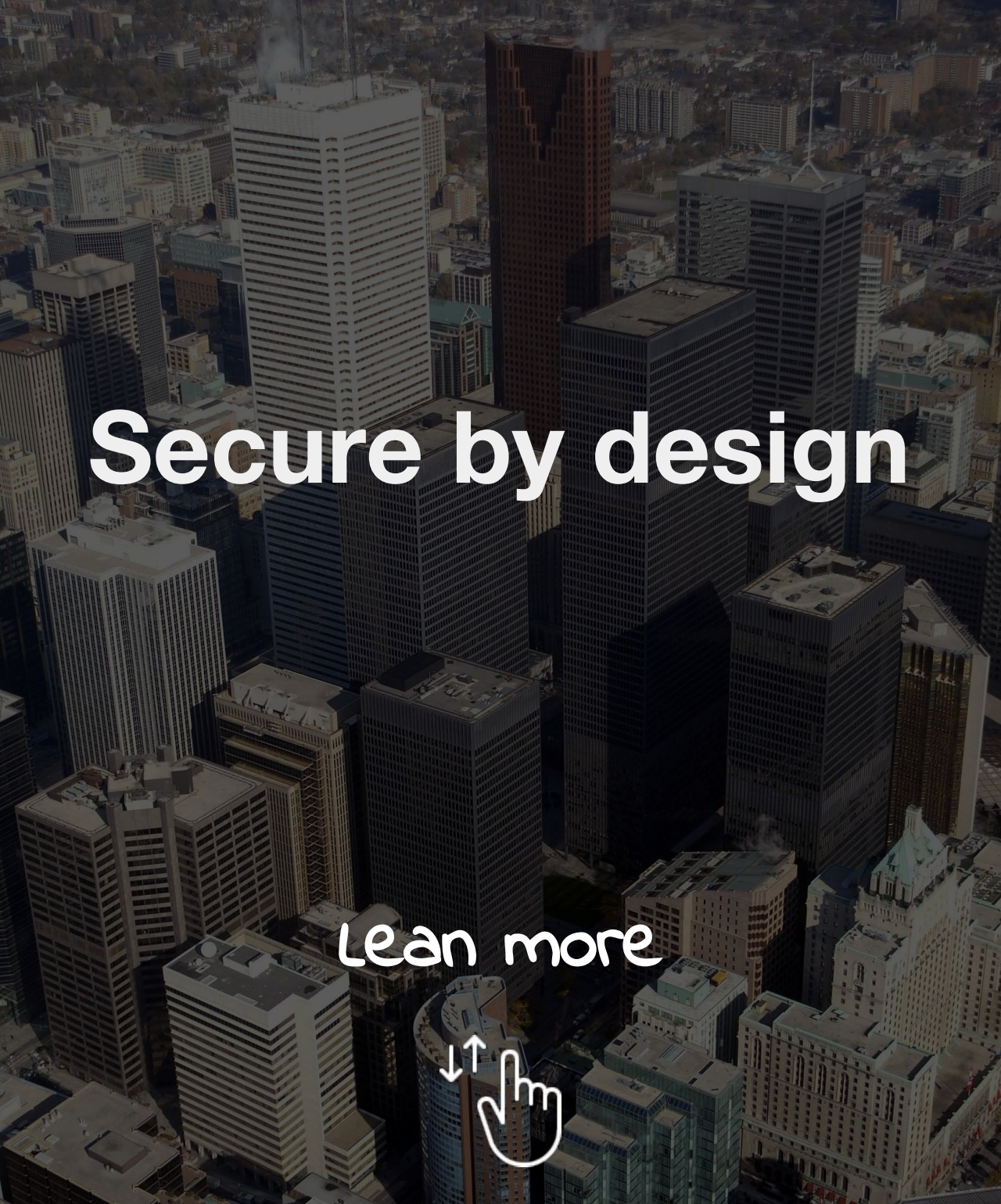
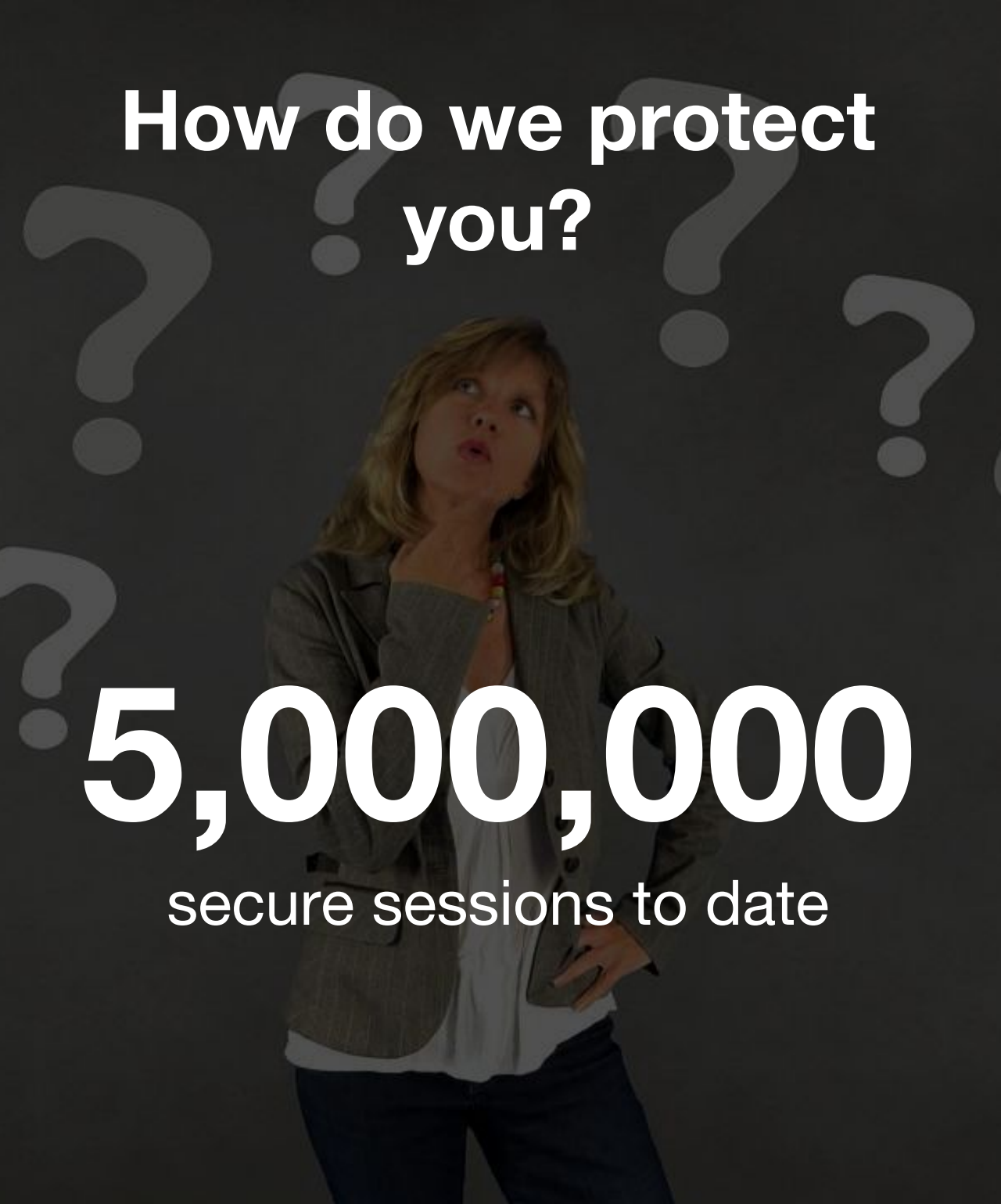

Secure by design
Lean more

How do we protect you?



5,000,000

secure sessions to date

Encryption & SSL

We encrypt your information and connection using AES 128 bit (Advanced Encryption Standard), a modern cipher encryption that offers data authenticity (integrity) and confidentiality.

The best two combinations.

In fact, the U.S. Government declared in 2003 that the AES algorithm is sufficient to protect classified information up to the **SECRET** level.

Physical Security

Our third party cloud infrastructure is hosted and managed within Amazon's secure data centres in the Canadian region.

These data centers provide a 4-layered security approach comprising of perimeter (fencing, intrusion detection), infrastructure (backup power, fire-suppression), environmental (flooding & seismic protection) and lastly data level protection by restricting access and providing separation of privileges between the layers.

App Transport Security

App Transport Security is a new feature built into iOS 9+

Specifically, we disallow:

- Unencrypted HTTP network connections
- HTTPS connections using old and insecure versions of SSL/TLS
- HTTPS connections using cipher suites that don’t provide forward secrecy
- HTTPS certificates that use insecure hash functions for their digital signatures

Access Control

Our infrastructure utilizes a combination of firewalls and internally implemented authentication schemes to restrict access to systems from external networks and between systems internally.

By default all access is denied and only explicitly allowed ports and protocols are allowed based on business needs.

Data Privacy

Your data being stored is securely managed by state-of-the-art infrastructure coupled with authentication measures right here in Canada.

It is fully managed by us with round the clock logging and access control measures that restrict both external and internal data usage unless explicitly advised.

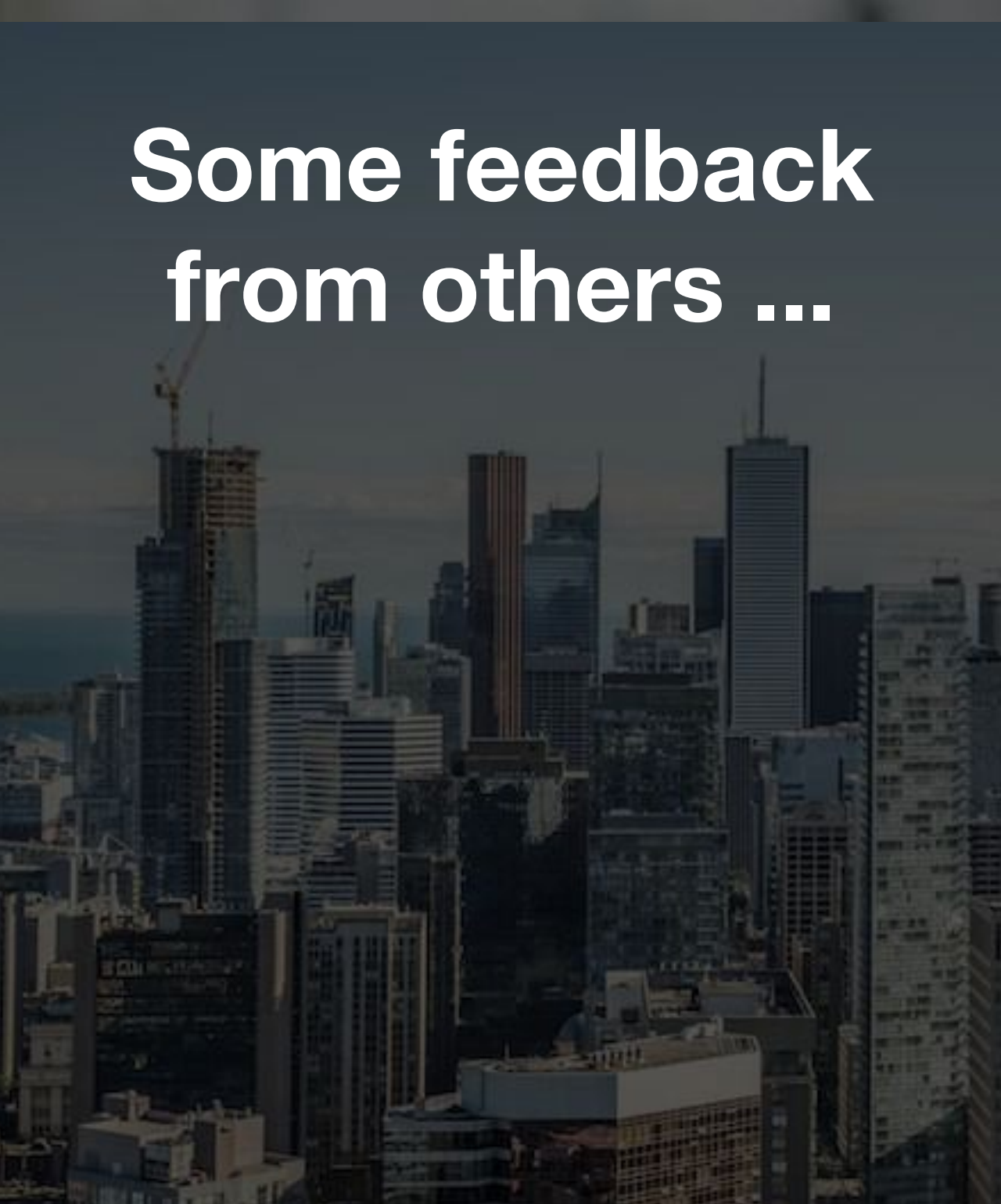
DDoS Mitigation

Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth.

Spoofing and Sniffing Protections

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Our backend platform provides service isolation, operating system restrictions, and encrypted connections to further enhance risk mitigation at all levels.

Some feedback from others ...



The most popular mortgage app in Canada

★★★★★ 2,827 Ratings

★★★★★ 1,753 Ratings

Well received by the media

“the app everyone loves to talk about when it comes to mortgages”

FINANCIAL POST

CANADIAN MORTGAGE TRENDS.com

CMA CANADIAN MORTGAGE AWARDS

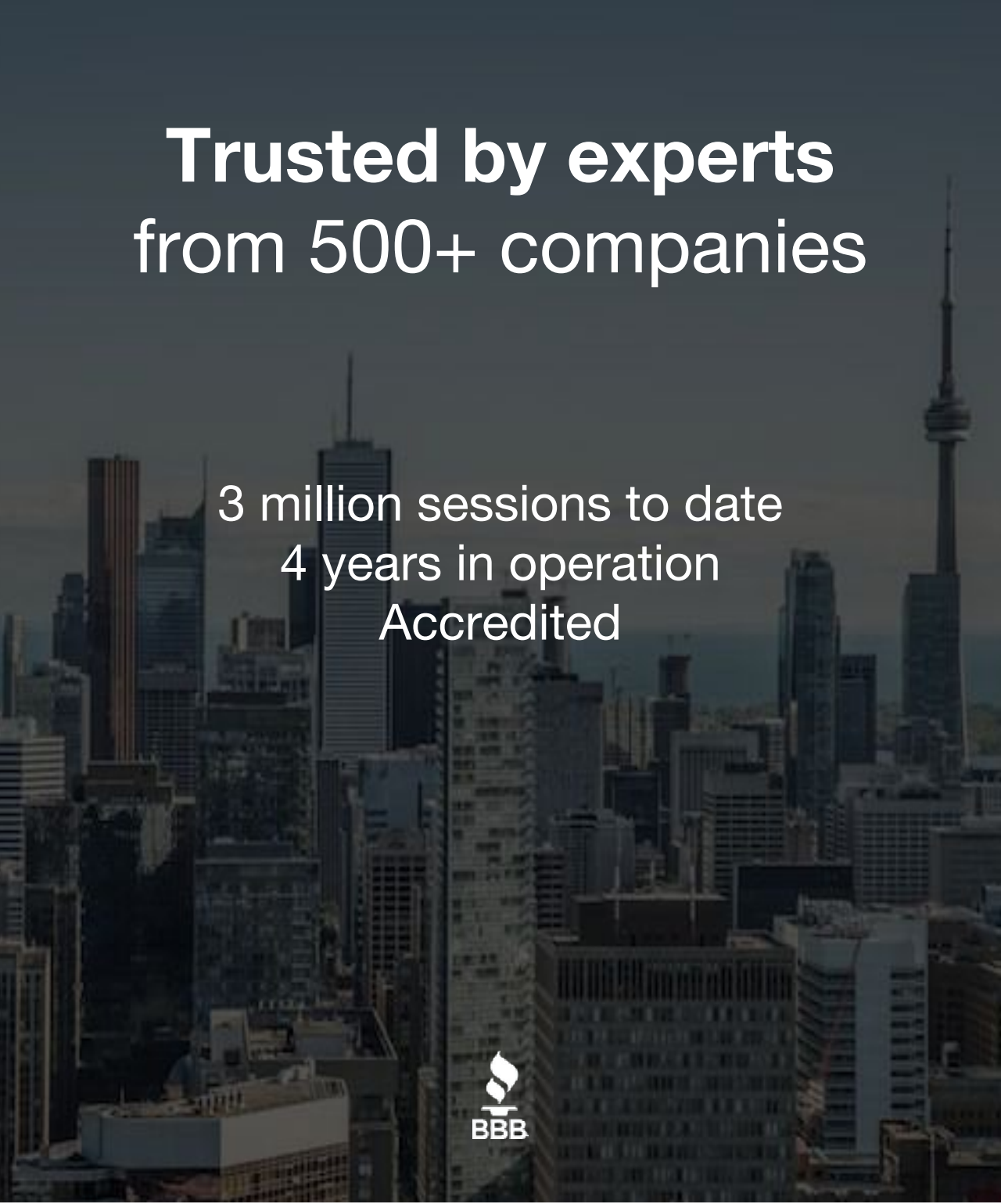
MORTGAGE BROKERNEWS.ca

LA PRESSE+

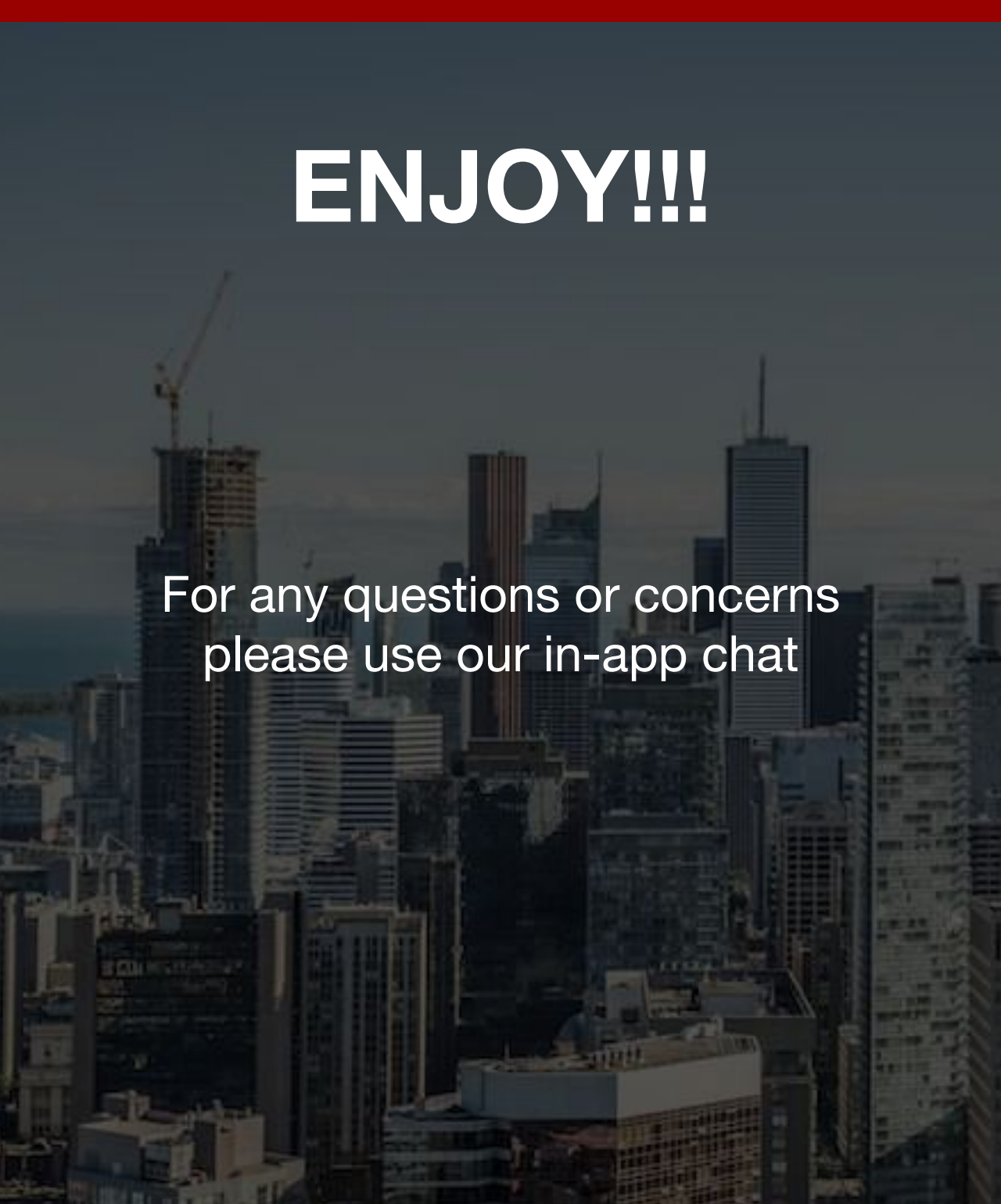
Well maintained with **Apple** and **Google**

Supports 8,000 devices
Updated for every rule change

Nominated for 2016 Canadian Fintech Startup of the year


Trusted by experts
from 500+ companies
3 million sessions to date
4 years in operation
Accredited
BBB

ENJOY!!!



For any questions or concerns
please use our in-app chat