CHARTER PACIFIC CORPORATION LIMITED UPDATE

BIOMETRIC PATENTS

FAMILY OF PATENTS

The patent portfolio comprises the following families of patents which are registered in various jurisdictions around the world as set out below:

1. Remote entry system
2. A transmitter for transmitting a secure access signal
3. Enhancing the response of biometric access systems
4. Improving credit/debit card device security using biometrics
5. Password generator
6. Solenoid operated latching strike
7. Personalised Automobile Access
8. Unauthorised Use of Patents

1. Remote Entry System

This patent is a stand-alone biometrics management, self-enrolment system used on all biometrically enabled mobile devices and involves enrolling a user into a biometric access platform using a succession of biometric placements within a mobile device.

The 'stand-alone' biometrics platform provides self-contained and self-managed security solutions.

This patent relates to any mobile device or mobile phone, as they require the biometric template management internally to allow access to the device by only the authorised user, plus adding and deleting other authorised users.

Jurisdiction	Publication/Patent Number
Australia	2004301168
Australia	2009201293
Canada	2535434
China	ZL201110037781.8
United Kingdom	EP1661298
Belgium	EP1661298
France	EP1661298
Germany	EP1661298
Netherlands	EP1661298
United States	9,269,208
United States	8,266,442
United States	9,269,208
United States	9,665,705

2. A Transmitter for Transmitting a Secure Access Signal

Adding NFC (Near Field Communication) technology inside any mobile or portable device will enable cashless payment applications to be incorporated. The NFC technology is standard around the world and allows multiple devices, smartphones, tablets, and biometrics credentials to be used on the same payment platform.

This technology identifies the credit/debit card user/owner/holder through fingerprint or other biometric verification solutions such as iris, voice, face, vein etc. authentication and prevents access by anyone other than the credentialed user.

Jurisdiction	Publication/Patent Number
Australia	2008316289
Australia	2014240323
Europe	EP3270540
United States	10,685,353
United States	16/717,270

Update of patents following the issuance of the Notice of Allowance for Patent No. 16/717,270 by the US Patent Office on 8 January 2021:

- The original patent relates to a situation where a smartphone user can select between different payment modes (e.g. different credit cards) when performing a contactless payment transaction with biometric authentication. The smartphone has a plurality of proximity modules (with corresponding integrated circuits).
- The first continuation application (which has been allowed) relates to the same practical situation, but the claim language has been improved to more clearly cover known situations where infringement may be occurring in the market.
- The second continuation, which is under examination, pushes further with claim language improvements.
- The third continuation relates to a situation where a smartphone user can perform contactless operations (with biometric authentication) for both payment transactions and unlocking/starting a car.

3. Enhancing the Response of Biometric Access Systems

This patent combines voice and fingerprint biometrics to identify individuals without the need for a credit/debit card or token for banking transactions. The voice biometric signature simply locates the fingerprint template in the database which then grants access to the authorised user.

This process speeds up the database search for a biometric signature/identifier in the database in the computing device (e.g. mobile phone, tablet, payment terminals or ATM) by reducing the size of the database to be searched simply by inputting a voice code into the mobile phone. Multi-modal (Combination) biometrics is a security technology of the future.

Jurisdiction	Publication/Patent Number
United States	8,112,278

4. Improving Credit/Debit Card Device Security Using Biometrics

This patent combines credit/debit card and fingerprint to add personal identification of the credit/debit card or token.

Enrolling a user in a credit/debit card / biometric system (such as a biometric enabled mobile phone, tablet, payment terminal or ATM) by locally storing the biometric signature/identifier at the ATM in a memory location defined by the credit/debit card.

Jurisdiction	Publication/Patent Number
United States	8,620,039

5. Password Generator

This patent combines a dynamic password generator software algorithm to a fingerprint identification system which adds biometrics as another level of security to existing banking devices such as internet banking passcode toggles.

This device will generate a one-time dependent password upon matching a predetermined biometric signal such as a fingerprint. The proliferation of dynamic number generators suffers from the same security weakness as access and NFC credit/debit cards; there is no identification of who is using the credit/debit card or token. Biometric identification of the person using the dynamic number generator is a significant enhancement to securing access or log-in only for the authorised user.

Jurisdiction	Publication/Patent Number
Australia	2009200408
United States	8,458,484

6. Solenoid Operated Latching Strike

All existing electro-mechanical door systems require a large amount of voltage applied for unlocking to gain entry. This patent is a bi-stable mechanism that requires a very small pulse or voltage spike to activate and remain stable in both states, lock/unlock. Once in the open (unlocked) or closed (locked) state, this bi-stable lock will remain in that position forever, without any further voltage requirements. This system has lower power requirements and therefore can be operated by battery and integrate other circuitry such as RF and Bluetooth systems.

Jurisdiction	Publication/Patent Number
United States	7,472,934

7. Personalised Automobile Access

https://support.apple.com/en-au/HT211234

8. Unauthorised Use of Patents

There are a significant number of the largest companies in the world in in industries such as mobile communications, mobile payment applications and mobile payment platforms together with various banking applications and secure access applications in the automotive industry, data protection, government and health industries that are infringing one or more of the patents in the Company's patent portfolio.

COMMERCIALISATION

The patents have been granted and registered in various countries around the world for some time. However, it has only been in recent past that the Company has secured the legal rights and entitlements to patents and the technology that utilises those patents has become mainstream and ubiquitous in biometrically secured consumer products worldwide. The Company's patents are now in use worldwide by some of the largest technology companies in the world and ready for commercialisation.

The Company finds itself in a similar position as **CSIRO** did with its WiFi technology in the early 2000s that was being incorporated in chipsets manufactured by the world's largest manufacturers without paying license fees to **CSIRO**. **CSIRO** successfully enforced their patent rights on the chipset manufacturers and has received significant financial compensation.

The Company has engaged with some of the largest tech companies in the world to enable it to start the commercialisation of the two main patents, "Remote Entry System" and "A Transmitter For Transmitting A Secure Access Signal", together with other patents in the patent portfolio.

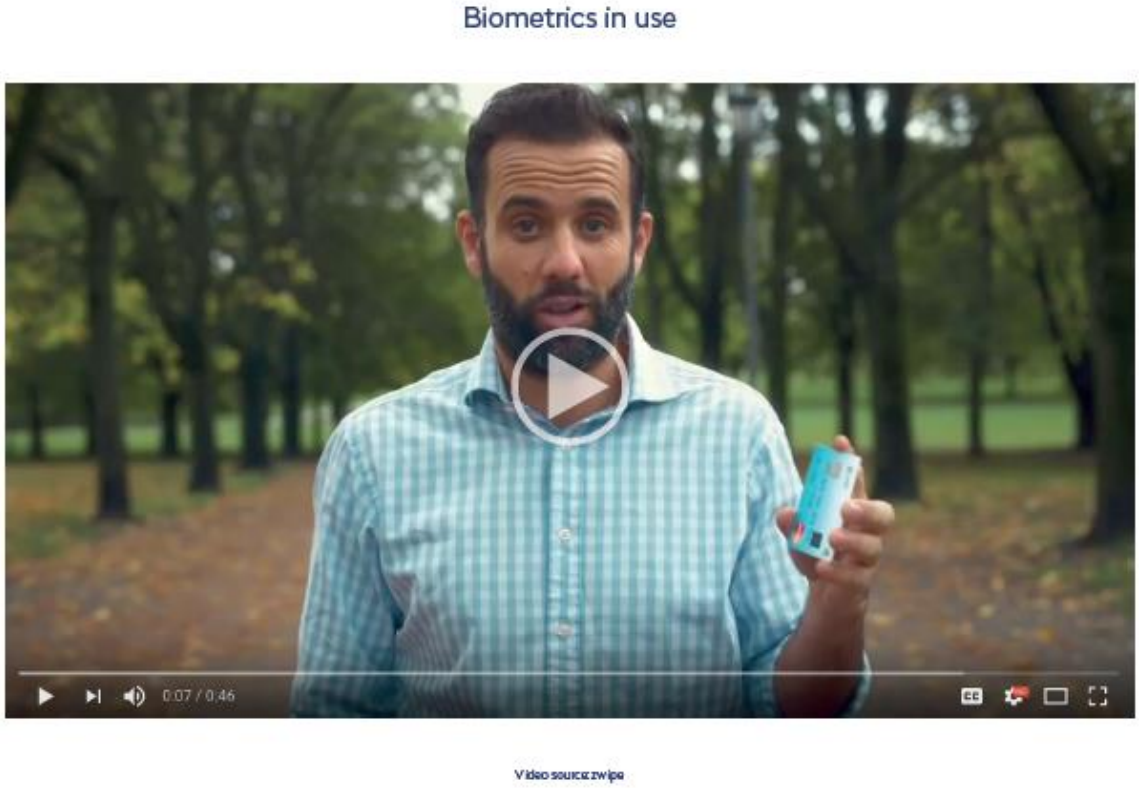
The most widely used patent is the "Remote Entry System" patent which has wide application on all remote/mobile computing devices such as smartphones, laptops, tablets and payment cards using biometrics as a security measure to ensure the integrity of the device and the data saved on and transacted with that device.

The business model for the Company is "Licencing and Sub-Licencing", "Development of Unique IP", "Partnerships" and "Acquisition Targeting" as follows;

- **Licencing or Sub-Licencing, Development of Unique IP and Partnerships**
  - Secure monthly/ annual licensing agreements with existing entities utilising our biometric technology
  - There are a number of known global entities which currently utilise our biometric patented technology.
  - Charter Pacific has plans to establish and accelerate license driven revenue growth through securing license agreements with companies using or planning to utilise the technology.
- **Strategic Partnerships**
  - Secure strategic partner agreements for the application of the biometric patents and technology (e.g. MasterCard or Visa who has credit cards)
- **IP Development**
  - Partner with manufacturers and providers to create and offer superior competitive solutions using biometric technology
- **Realise Patent Capital**
  - Explore third party acquisition of full patents

Litigation with some of the patent infringers will be unavoidable and it is intended that the Company will utilise any number of litigation funding methodologies to enforce its patent rights when necessary.

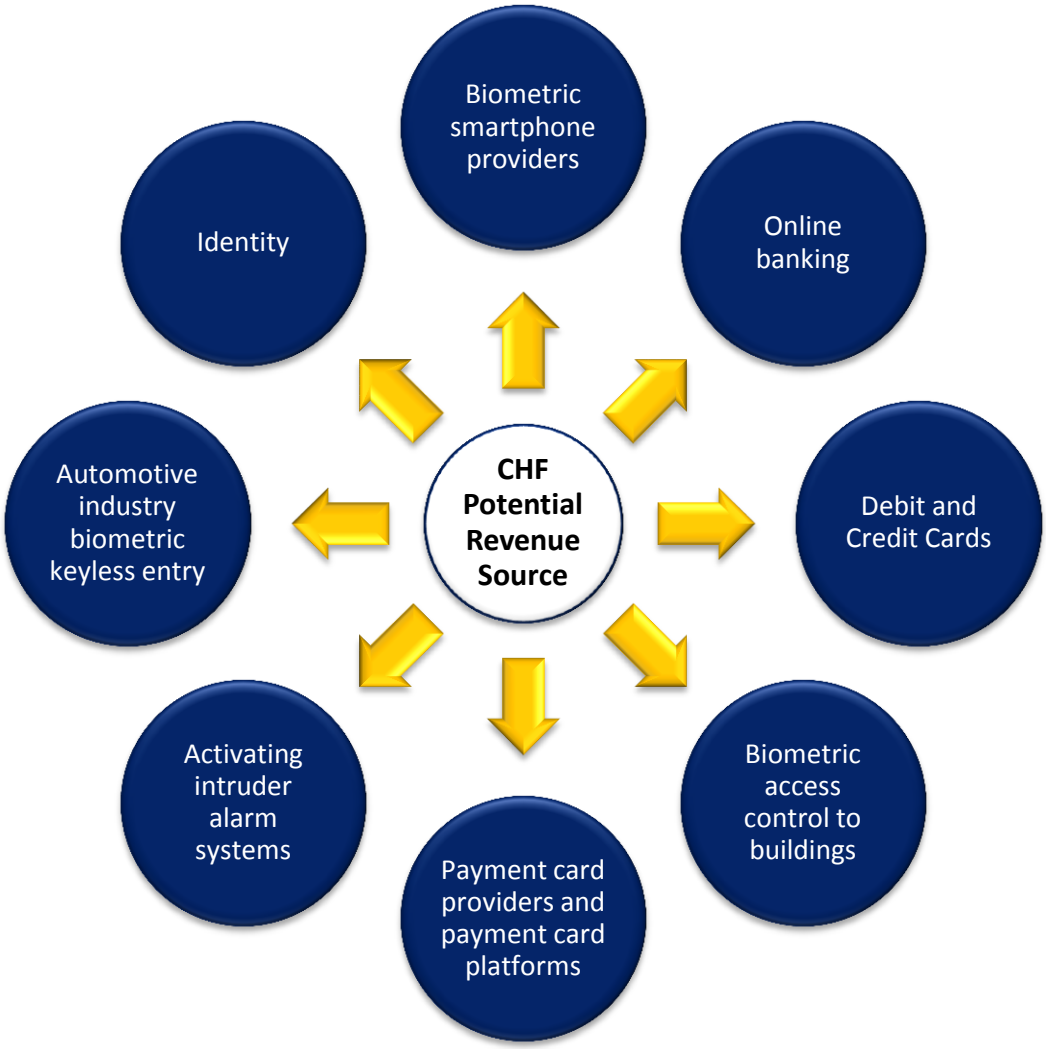
Biometrics in use



Video source: zwipe

https://www.youtube.com/watch?v=pjOxHrA5bj4

Key Applications for existing and future use of the biometric patents



Mobile computing device secure access
Secure biometric access.

Payment Card Providers and Platforms
Touchless payment transactions enabled by secure biometric access.

Debit and Credit Cards
Addition of biometric signature of authorised user on all debit and credit cards.

Online banking
Future addition/ replacement of Online banking One Time Password devices with biometric signature of authorised user.

Identity
Inclusion of biometric signature of authorised user on driver's licenses, passports and general corporate and/or government identification cards.

Personal Security
Biometric activation of intruder alarm systems replacing PIN.

Automotive
Addition of fingerprint biometrics to car remote key fobs to ensure that only the authorised user has access to the vehicle.

Security access (building and data networks)
Biometric access control to buildings, rooms and data networks for every entry / log-in application.

INDUSTRY BACKGROUND

Biometrics authentication is a user identification and verification process that uses unique physical and behavioural characteristics like fingerprint, iris, face, voice ID and palm vein.

Fingerprint recognition is a biometric process of electronically obtaining and storing human fingerprints for biometric authentication. It is the most widely used modality.

Iris recognition uses mathematical pattern recognition techniques of one or both irises of an individual's eye for identifying people based on unique patterns within the region surrounding the pupil of the eye.

Facial recognition is a biometric process of identifying and verifying a person by analysing and comparing patterns based on facial contours. Face biometrics has garnered high popularity in the past two years.

Voice ID is a biometric method of speaker recognition using vocal characteristics to uniquely identify users. This modality is commonly used for remote authentications.

Palm vein recognition is a biometric identification process based on the unique patterns of veins in the palm of people's hands.

Biometric authentication will be used to authenticate $2.5 trillion in mobile payments by 2024, an increase of nearly 1,000 percent from $228 billion in 2019, driven by the rise of WebAuthn standards adoption, according to a new report from Juniper Research.

The Mobile Payment Authentication & Data Security: Encryption, Tokenisation, Biometrics 2019-2024 report suggests that 90 percent of smartphones will have dedicated biometric hardware by 2024, but less than 30 percent of them to be used to authenticate contactless payments, due to the use of contactless cards. Due to the Covid 19 pandemic in 2020 there has been a sharp increase in the use in biometric authentication of contactless payments in the last 12 months.

The tokenization for contactless and remote payments using fingerprint, facial, iris, and voice biometric modalities is becoming ubiquitous globally and is rapidly being taken up in key regions and important emerging country markets in Asia, South America and Africa.

Biometrics has traditionally been used for in-person contactless payments; however, with an increase in the need for smooth authentication on all mCommerce channels and Covid 19 conditions prevailing, researchers anticipate that over 60 percent of biometrically-verified payments will be made remotely by 2024.

Statistica reported in November 2020 that total eRetail transaction values will reach US$6.54 trillion by 2023, up from US$3.53 trillion in 2019.

The research identified Chinese eRetail market as a major factor, as well as regions such as Latin America, Africa and Middle East, as improvements in connectivity will enable the rise of eRetail in new markets.

The research also found that mobile handset penetration is rising faster than banking penetration in developing markets, meaning that mobile access is the best way for eRetail and payments providers to reach potential users. The safest and most effective security for such devices is biometric authentication.