Anatomy of a Ransomware Attack

Today's Session

- The Threat Landscape
- Anatomy of a Ransomware Attack
- Identifying Your Risk
- Mitigation Strategies
- Q&A

DATABOX + HEALTH

The Threat Landscape — Key Statistics

- In 2024, 41% of healthcare organisations in Australia experienced a cyber attack
- Most common causes: phishing (34%), ransomware (28%), compromised credentials (18%)
- Average cost of a data breach in Australia: $3.35 million
- 1,549 notifiable data breaches reported in 2024 — up 26% from 2023

Healthcare Breaches — By the Numbers

Why Healthcare Is a Prime Target

- 200+ data breach notifications from health service providers in a single 12-month period
- Over 90% of healthcare breaches involved personally identifiable information (PII)
- Patient names, Medicare numbers and health records are the most commonly stolen data

Key Trends

- 71% year-on-year increase in cyber attacks targeting healthcare organisations globally
- Ransomware accounted for 11% of all healthcare cyber incidents in 2023–24, with compromised accounts at 32%

Real-World Cases

Australian Clinical Labs — $5.8M Penalty (Oct 2025)

Federal Court imposed a $5.8M civil penalty on one of Australia's largest pathology providers for systemic failures that led to the unauthorised access and theft of data belonging to 223,000+ individuals.

Pound Road Medical Centre, VIC (Feb 2025)

Ransomware group "Anubis" leaked passports, dates of birth and medical records. The practice confirmed the breach and directed affected patients to Services Australia to protect their Medicare and myGov accounts.

General Landscape

Threat Type	Description	Potential Impact	Key Mitigations
Ransomware	Malware locks or encrypts patient data until a ransom is paid.	Disruption to patient care, data loss, reputational damage.	Regular backups, patch management, staff training, endpoint protection.
Phishing / Spear Phishing	Fake emails or texts trick staff into revealing passwords or downloading malware.	Unauthorised access, financial fraud, data breaches.	Staff awareness training, email filtering, multi-factor authentication (MFA).
Data Breaches	Unauthorised access or theft of patient or financial data.	Privacy violations, regulatory fines, legal liability.	Access controls, encryption, incident response plan, compliance monitoring.
Insider Threats	Malicious or careless staff misuse data or systems.	Data leaks, privacy breaches, internal disruption.	Role-based access, monitoring, staff policies, offboarding controls.
Malware / Spyware	Hidden software steals data or monitors system activity.	Credential theft, identity fraud, compromised systems.	Antivirus tools, software updates, restricted admin rights.
Network Intrusions	Hackers exploit vulnerabilities or weak passwords.	Data loss, system downtime, compromised infrastructure.	Strong passwords, firewalls, intrusion detection, regular audits.
Social Engineering	Attackers impersonate staff, vendors, or patients.	Unauthorised access, fraud, data exposure.	Verification procedures, staff awareness, access protocols.
Fraud & Identity Theft	Stolen patient or Medicare data used for fake claims or identities.	Financial loss, patient trust damage, compliance risk.	Data minimisation, encryption, fraud monitoring.
Denial of Service (DoS)	Systems overloaded with traffic, causing shutdowns.	Disrupted online services (telehealth, bookings).	Cloud-based DDoS protection, network resilience.
Supply Chain Attacks	Compromise of third-party IT or software providers.	Indirect data exposure, system compromise.	Vendor vetting, contractual security clauses, regular risk reviews.

Anatomy of a Ransomware Attack

A real-world case study from an Australian medical practice

Timeline Overview

Back Story

- Relied on a single IT contractor using a break-fix model
- Very limited investment in hardware and software
- Complacent about the risk to their business and patients' data
- Turned down multiple recommendations to bring the environment up to standard
- Sub-par backup strategy
- No multi-factor authentication
- Reused passwords across accounts

Stage 1 – Initial Compromise

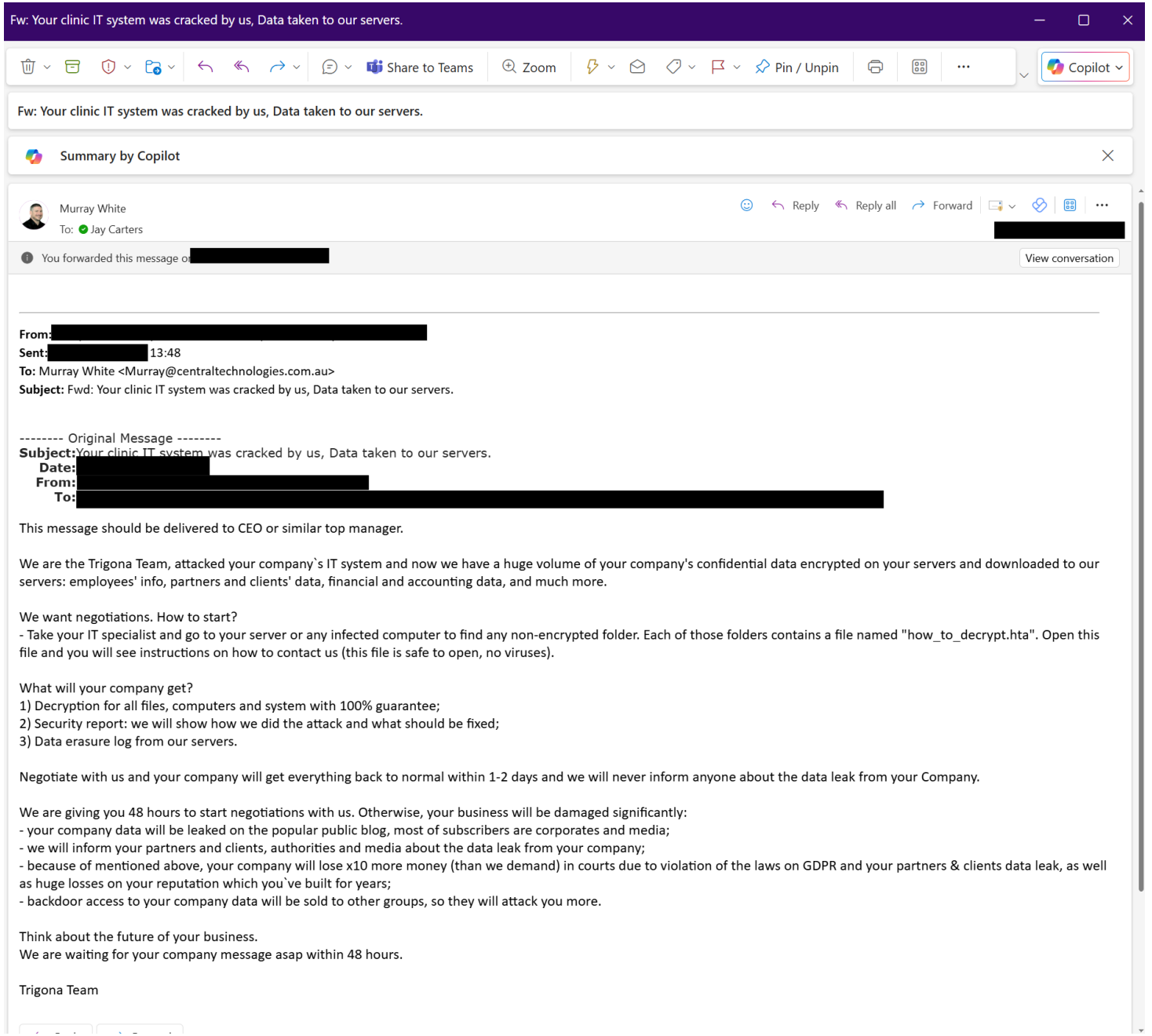
How were they compromised:

- Compromised email account via phishing
- Admin password compromised — same password reused for email
- No VPN in use — open ports on the router exposed the network / server to the internet

Stage 2 – System Lockout

- Staff arrived at 6:30 am to find all files and Best Practice inaccessible — first patients due at 7:00 am
- No business continuity plan in place for a system outage
- Forced to use paper records, then ultimately close the doors to patients
- Immediate impact on revenue and enormous stress on staff

Stage 3
Ransom Demand



Fw: Your clinic IT system was cracked by us, Data taken to our servers.

Share to Teams | Zoom | Pin / Unpin | Copilot

Fw: Your clinic IT system was cracked by us, Data taken to our servers.

Summary by Copilot

Murray White
To: Jay Carters

Reply | Reply all | Forward

You forwarded this message o[redacted]

View conversation

From: [redacted]
Sent: [redacted] 13:48
To: Murray White <Murray@centraltechnologies.com.au>
Subject: Fwd: Your clinic IT system was cracked by us, Data taken to our servers.

-------- Original Message --------
Subject: Your clinic IT system was cracked by us, Data taken to our servers.
Date: [redacted]
From: [redacted]
To: [redacted]

This message should be delivered to CEO or similar top manager.

We are the Trigona Team, attacked your company`s IT system and now we have a huge volume of your company's confidential data encrypted on your servers and downloaded to our servers: employees' info, partners and clients' data, financial and accounting data, and much more.

We want negotiations. How to start?
- Take your IT specialist and go to your server or any infected computer to find any non-encrypted folder. Each of those folders contains a file named "how_to_decrypt.hta". Open this file and you will see instructions on how to contact us (this file is safe to open, no viruses).

What will your company get?
1) Decryption for all files, computers and system with 100% guarantee;
2) Security report: we will show how we did the attack and what should be fixed;
3) Data erasure log from our servers.

Negotiate with us and your company will get everything back to normal within 1-2 days and we will never inform anyone about the data leak from your Company.

We are giving you 48 hours to start negotiations with us. Otherwise, your business will be damaged significantly:
- your company data will be leaked on the popular public blog, most of subscribers are corporates and media;
- we will inform your partners and clients, authorities and media about the data leak from your company;
- because of mentioned above, your company will lose x10 more money (than we demand) in courts due to violation of the laws on GDPR and your partners & clients data leak, as well as huge losses on your reputation which you`ve built for years;
- backdoor access to your company data will be sold to other groups, so they will attack you more.

Think about the future of your business.
We are waiting for your company message asap within 48 hours.

Trigona Team

Stage 4 – Response & Containment

- The outgoing IT provider handled the initial response
- They restored a 7-day-old backup, then refused to do any further work
- The practice was left with a barely functioning environment
- No action was taken to secure the environment going forward

Turning Point — The Call for Help

- The practice manager reached out to Murray, based on earlier conversations and asked if we would consider taking on their business and helping them recover.
- We attended the practice and began work the same day.

Stage 5 – Restoration of Services

- Physically disconnected from the internet during restoration
- Rebuilt the server environment from scratch and imported BP data
- Commenced local and cloud backups daily
- Rebuilt all workstations from scratch; restored access to shared files
- Installed monitored security software on all devices

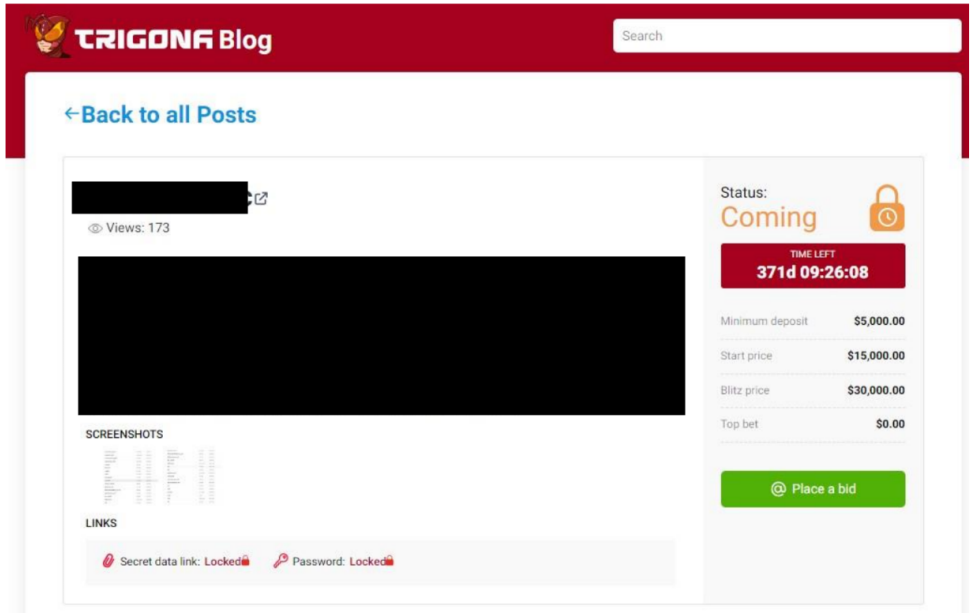
Stage 5 — What We Uncovered

- During restoration, several additional IT and security issues were uncovered
- These were collated into a comprehensive remediation proposal covering all outstanding IT and cyber security concerns
- The scope of the required upgrades highlighted years of underinvestment in critical infrastructure and security

Stage 6 – Forensic Investigation

Following service restoration, the practice engaged forensic specialists to confirm the scope of the attack and determine whether data had been stolen.

The analysis confirmed that patient data had been exfiltrated and was, in fact, for sale on the dark web.



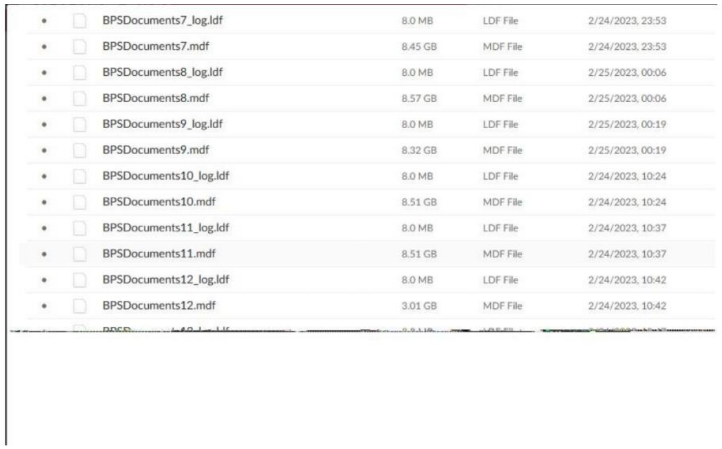


Figure 2: Screenshot 1.

Stage 7 – Legal & Regulatory Response

- Required to notify all patients under the Notifiable Data Breaches scheme (Privacy Act 1988)
- Email sent to the entire patient database disclosing the breach and loss of personal data
- Formal notification lodged with the Office of the Australian Information Commissioner (OAIC)

Lessons Learned

Years of underinvestment in IT security led to a devastating financial, operational, and reputational impact.

The repercussions included:

- Unable to operate at full capacity for many days
- Cost of forensic analysis and IT recovery services
- Loss of patients and damage to reputation
- Significant investment required to bring the IT environment up to standard
- Non-compliance with Essential 8 and RACGP guidelines

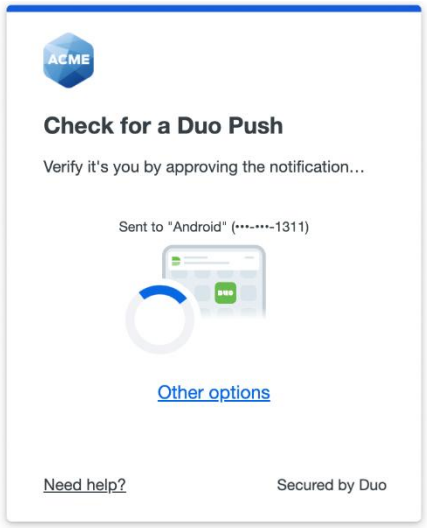
Identifying Your Risk – Firewalls & Perimeter

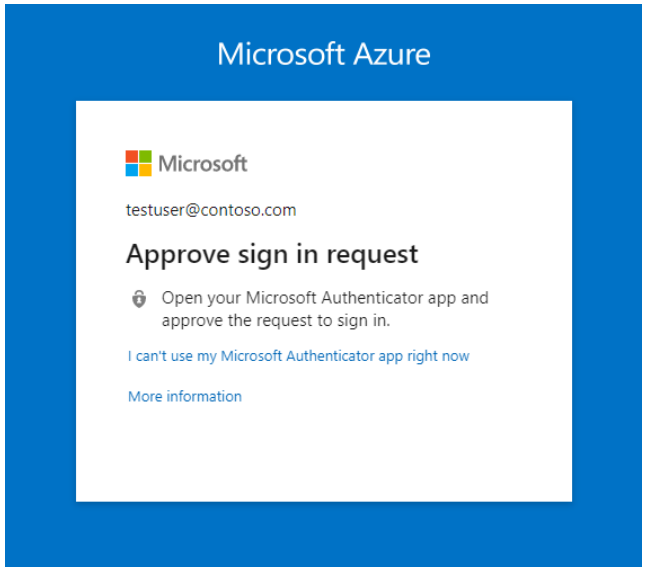
Identifying Your Risk – VPN & Remote Access

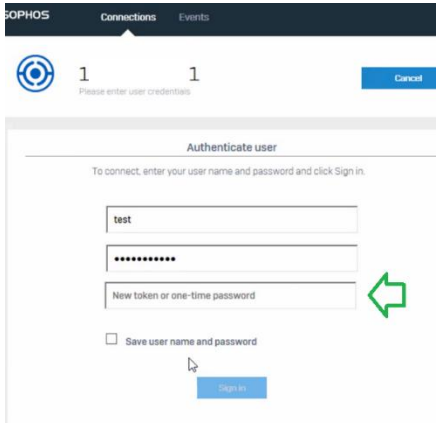
Identifying Your Risk – NGFW vs Standard Router

Feature	Next-Gen Firewall (NGFW)	Standard Modem / Router
Main Role	Security and threat prevention	Internet connectivity
Protection Level	Advanced – blocks viruses, ransomware, and hacking attempts	Basic – minimal firewall only
Traffic Inspection	Deep inspection of all data packets	Only checks where data is going/coming from
User & App Awareness	Identifies users and controls access by application	No visibility of users or apps
Threat Updates	Uses live threat intelligence feeds	No real-time updates
Best For	Businesses needing secure, monitored networks	Home or small offices with basic needs

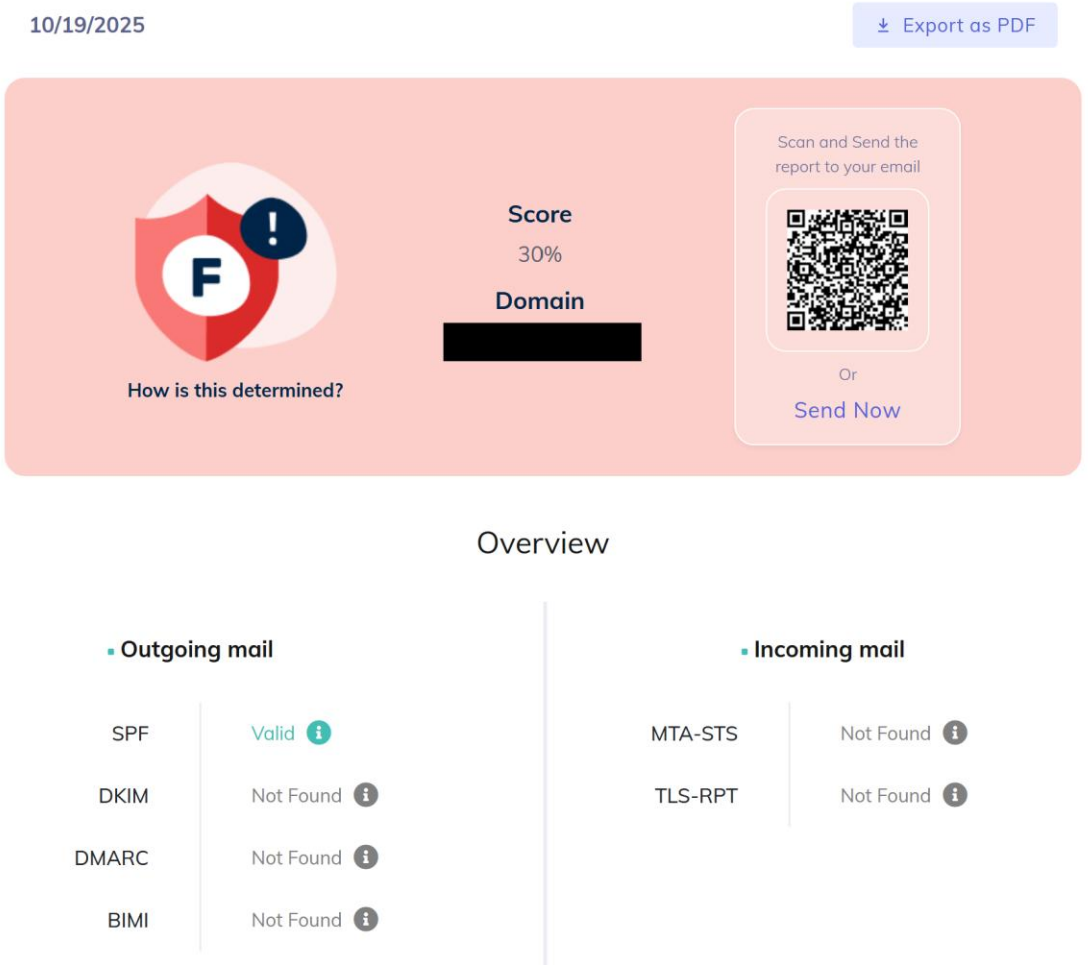
Identifying your Risk – Multi-Factor Authentication







Identifying your Risk – Email Security



Identifying your Risk – Health Check

- Scan the QR code or visit our booth for a free copy of our comprehensive Cyber Security Questionnaire. This can be forwarded to your existing IT provider to complete.
- This questionnaire is based on the Australian Government's Essential 8, the RACGP's Information Security standards (Criterion 6.4), and our own experience securing medical practices and assisting in recovery from cyber attacks.

Mitigation Strategies

- Audit your environment regularly against Essential 8 and RACGP standards
- Use a proper firewall — not just a router — and require VPN for all remote access
- Deploy a secure email solution with MFA on all accounts; monitor and protect your domain names
- Choose proactive managed IT services over break-fix providers — hold them accountable with regular reports
- Train staff regularly on the latest threats and social engineering tactics

About Us

- Databox Health delivers positive outcomes and real-world improvements for healthcare partners across Australia
- Fully managed IT services with 100% Australian-based support
- Cyber security consulting — including audits, disaster recovery, and comprehensive technology overhauls
- Partnered with leading software and hardware providers
- ISO certified for security and quality

DATABOX + HEALTH

Q&A

Thank you