



ISI-2026-1002

Mailbox access on the Exchange server

STATUS

OPEN

SERIOUS

AVENUE OF ATTACK	Software vulnerability — as assessed by the operator
OCCURRED	3 Oct 2026, 02:14
NOTICED / OPENED	6 Oct 2026, 09:20
CONTAINED	Not confirmed contained
DWELL	12 days between the incident occurring and being contained

What the operator recorded

The GM noticed replies to emails he never sent. On-prem Exchange 2019, server has not been patched since we installed it. Looks like ProxyLogon to me (CVE-2021-26855) — it is the one that hits unpatched Exchange and it is internet facing. Assuming full mailbox compromise until shown otherwise.

In summary

Between 2 and 3 October an external actor sprayed credentials against the mail server's web services interface and succeeded in authenticating as the General Manager, who had reused his warehouse-portal password and whose account was not protected by multi-factor authentication because of a legacy exclusion. The attacker then accessed the mailbox over several hours. The incident was first noticed on 6 October when the GM saw replies to messages he had not sent; eleven days on, the server is not confirmed contained, and the scope of what was read, exfiltrated or altered has not been established. The operator's initial theory of a ProxyLogon exploit against an unpatched server is not supported by the evidence: the build is current and the log pattern is credential abuse, not exploitation.

Does this look notifiable?

Opinion only: this should be treated as notifiable and the clock assumed to have started on 6 October. The compromised mailbox belongs to a senior officer and the questionnaire records that customer personal data, commercial material and credentials could all have been reachable. Until mailbox audit data is pulled and the content of the mailbox is characterised, the organisation cannot credibly tell a regulator that personal data was not accessed, and the safer regulatory posture is to notify on the assumption that it was.

An opinion formed from the evidence on the record, not a legal determination.

Control measures in this report are described in plain language and are not mapped to any named standard or framework. Evidence on this incident is append-only — corrections and withdrawals add to the record rather than replacing it — so this document can be reproduced exactly as it reads today at any future date.

HOW TO READ THIS DOCUMENT

Prepared with ISI, an incident recording and analysis tool operated by WebGen Services Pty Ltd. It works only from the information entered against this incident and can be no more complete than that information. Nothing in it is legal, regulatory or professional advice, and no part of it is an expert opinion or a determination — including any comment on whether the incident appears notifiable. It is a working resource to be interpreted by someone competent to do so, as one input to a wider investigation. Questions: webgen@webgen.com.au.

What was found and what to do

12 of 12 actions outstanding. 4 of them remove the exposure rather than reducing the damage.

Now

DONE	ACTION	WHAT IT ACHIEVES
☐	Disable basic authentication on EWS and IMAP and remove the legacy exclusion Turn off basic auth on EWS and IMAP at the server, delete the 2023 exclusion entry entirely rather than narrowing it, and confirm conditional access / MFA now covers every remaining authentication path to the mailbox service. If the stocktake scanner still exists, move it to a modern auth flow or a service account with its own compensating controls.	REMOVES THE EXPOSURE
☐	Produce a written containment checklist and complete it Record, with timestamps, the password reset, token and session revocation, basic auth disablement on EWS and IMAP, removal of the MFA exclusion, IP blocks, rule and forwarder purge, and any server-side cleanup. Attach the evidence (portal screenshots, PowerShell output) to each item.	REMOVES THE EXPOSURE
☐	Force a password reset and session/token revocation for g.mertens and any other account seen with a 200 from the /24 Reset the credential server-side (not just a user-chosen change), revoke all existing sessions and refresh tokens, and verify the reset took effect before re-enabling access. Pull the full set of 200 responses from 203.0.113.0/24 between 1 October and now and apply the same treatment to every username that appears.	REMOVES THE EXPOSURE
☐	Enumerate and purge rules, transport rules and forwarders List inbox rules on g.mertens, tenant-level transport rules, and any SMTP forwarders created or modified since 3 October. Remove anything the attacker placed and record what was there before removal.	REMOVES THE EXPOSURE
☐	Block the known attacker source ranges at the edge Block 203.0.113.51 and the wider 203.0.113.0/24 at the perimeter or on the mail publishing path pending investigation of the ASN and geolocation.	REDUCES THE DAMAGE
☐	Pull and review mailbox audit data for g.mertens Run Search-MailboxAuditLog for g.mertens for 1 October onwards, specifically looking at MailItemsAccessed, Send, SendAs, Move, HardDelete, rule changes and folder permission changes. Preserve the output as evidence.	MAKES IT VISIBLE NEXT TIME

Within days

DONE	ACTION	WHAT IT ACHIEVES
☐	Characterise the content of the mailbox Produce a defensible estimate of what categories and volumes of data were in the mailbox during the exposure window — customer personal data, contracts, any cleartext credentials — to inform notification decisions and credential-rotation scope.	MAKES IT VISIBLE NEXT TIME
☐	Confirm the server is clean beyond the mailbox Review the mail server for web shells, scheduled tasks, new local accounts and unexpected modules even though the entry vector appears to be credential abuse rather than code execution — this provides the evidence to say containment is complete.	MAKES IT VISIBLE NEXT TIME

☐	Decide and record the external notification position Make and record a decision on notifying the insurer, the relevant regulator, affected customers and the MSP in writing, with the reasoning. The questionnaire currently shows no answer to who has been told.	RESTORES WHAT WAS LOST
--------------------------	--	------------------------

Within weeks

DONE	ACTION	WHAT IT ACHIEVES
☐	Deploy password-reuse and breached-password checks for staff accounts Enforce a check at password-set time against known-breached credential corpora, and give senior and privileged users guidance (and a password manager) to prevent reuse against third-party sites like the warehouse portal.	REDUCES THE DAMAGE
☐	Maintain an accurate, queryable inventory of internet-facing systems and their patch state Record for each internet-exposed service the product, exact build, last update applied, and authentication configuration, and refresh it on a schedule. In an incident, this is what triage reads from, rather than memory.	MAKES IT VISIBLE NEXT TIME
☐	Introduce alerting on authentication failure patterns against the mail server Instrument the IIS logs (or an equivalent source) so that a burst of 401s across multiple usernames from one source, or a 200 immediately following such a burst, raises an alert in hours rather than being noticed by a user eleven days later.	MAKES IT VISIBLE NEXT TIME

FINDING 1 OF 4 · SERIOUS · 85% CONFIDENCE

Entry was password spray landing on a reused password, not a server exploit

The operator's working theory is ProxyLogon against an unpatched Exchange 2019. The evidence does not support that. Get-ExchangeServer and ExSetup.exe both report build 15.2.1544.4, which is Exchange 2019 CU14 from February 2024 — years after the ProxyLogon fix. The IIS logs show roughly 1,400 401 responses across 41 distinct usernames from a single /24 on 2 October, followed on 3 October by clean 200 responses for g.mertens from one address in that same /24, with no 500s and none of the URI shapes associated with ProxyLogon or related SSRF chains. That pattern is credential spraying succeeding against one account. The GM has stated that the password on that account was reused from the warehouse portal. The incident should be worked, and reported, as account compromise via credential abuse.

Rests on 4 items of evidence — see the dossier in Appendix B.

CONTROL MEASURES IMPLICATED

IN PLACE AND GOT AROUND **Multi-factor authentication on all remote mail access paths** — MFA was in place for OWA and ActiveSync but a tenant-level exclusion from 2023, originally made for a stocktake scanner, left EWS and IMAP accepting basic authentication without MFA and outside conditional access. The GM's account fell inside that gap. Rebuilding MFA generally does not fix this; the exclusion itself is the control failure.

NOT IN PLACE **Prevention of password reuse between corporate and third-party accounts** — The GM reused his warehouse-portal password for his corporate mailbox. There is no evidence of any enforcement, detection or user guidance that would have surfaced this before an attacker did.

NOT IN PLACE **Detection of authentication brute force and spray against the mail server** — Approximately 1,400 failed logins across 41 usernames from one /24 in a short window produced no alert and no automated lockout or source-IP block. The attempt was only visible retrospectively in IIS logs after the GM noticed sent replies.

FINDING 2 OF 4 · SERIOUS · 80% CONFIDENCE

Scope of mailbox access, exfiltration and persistence is still unknown

The operator is working to the assumption of full mailbox compromise, which is a reasonable posture but is not yet a finding. The IIS log confirms four successful EWS POSTs as g.mertens on 3 October between 02:14 and 06:51, but no mailbox audit log, MailItemsAccessed data, Sent Items review, inbox rule enumeration, transport rule enumeration or SMTP forwarder check has been produced. The actual content of the mailbox — volumes of customer personal data, contractual material, any cleartext credentials — has also not been characterised. Without this, the organisation cannot describe what was read, what was sent, whether a forwarding or rule-based persistence mechanism remains in place, or what regulatory and contractual notifications are owed.

Rests on 2 items of evidence — see the dossier in Appendix B.

CONTROL MEASURES IMPLICATED

NOT ESTABLISHED

Mailbox and admin audit logging sufficient to reconstruct account activity after the

fact — Whether mailbox audit logging and MailItemsAccessed were enabled on g.mertens before the incident, and for how long logs are retained, has not been confirmed. If they were not enabled, the ability to answer scope questions is permanently reduced.

NOT IN PLACE

Enumeration of mailbox rules, transport rules and forwarders as part of incident

response — Eleven days after discovery, the standard set of persistence checks for a compromised mailbox has not been run or produced.

FINDING 3 OF 4 · SERIOUS · 75% CONFIDENCE

Containment is not confirmed and response actions since 6 October are not evidenced

The incident record shows the matter is not contained and dwell is counted at eleven days. The GM states he has changed the reused password. Beyond that, there is no evidence that sessions and tokens have been revoked, basic authentication has been disabled on EWS and IMAP, the MFA exclusion has been removed, the attacker IPs have been blocked, or mailbox rules have been checked and purged. A user-driven password change alone does not evict an attacker who holds a valid session token or who has planted a forwarding rule.

Rests on 2 items of evidence — see the dossier in Appendix B.

CONTROL MEASURES IMPLICATED

NOT IN PLACE

Documented incident response actions with timestamps and operator

— The questionnaire records every containment-relevant action as unanswered. There is no written record of what was done, when, or by whom since 6 October.

Operator's initial diagnosis is not supported by the evidence and should be withdrawn

The operator opened the incident attributing it to a software vulnerability, specifically ProxyLogon (CVE-2021-26855), on the stated basis that the server had not been patched since installation. Two pieces of evidence contradict this. First, build 15.2.1544.4 corresponds to Exchange 2019 CU14, released in February 2024, which is well after the ProxyLogon fix — the server is not at install-time patch level, and is not vulnerable to that CVE. Second, the IIS logs show the signature of credential spraying followed by a successful logon, not the request patterns associated with ProxyLogon exploitation. The report records this because an incident worked on the wrong theory produces the wrong remediation: hardening the server against a bug it does not have will not address a reused password behind an MFA exclusion.

Rests on 2 items of evidence — see the dossier in Appendix B.

CONTROL MEASURES IMPLICATED

IN PLACE BUT INADEQUATE

Baseline knowledge of patch state and architecture of internet-facing systems — The operator's recollection of patch state (never patched since install) was wrong by multiple years. Decisions in the first hours of an incident were being made against a mental model of the environment that did not match reality.

Still not established

- What the attacker actually did inside the mailbox — no Search-MailboxAuditLog, MailItemsAccessed, Sent Items review, rule/forwarder enumeration or folder-permission check has been produced, so the scope of read, send and persistence actions is unknown.
- Whether any other accounts were successfully authenticated from the same /24 — the log extract shown only confirms 200s for g.mertens, but the full set of 200s across the window has not been pulled.
- Whether the attacker still has access — no password reset timing, token/session revocation, basic-auth disablement, exclusion removal or IP block has been evidenced; the GM says he changed the password but the server-side state is not confirmed.
- What is actually in the mailbox — customer PII volumes, contract material, and whether any cleartext credentials are sitting in it — which drives both notification scope and secondary exposure.
- Where else the reused password was valid, and whether all those places have been rotated.
- Whether anyone outside the business (insurer, regulator, affected parties, MSP in writing) has been notified yet.
- Whether anything (WAF, reverse proxy, geo-filter) sits in front of the server — relevant to both how the spray reached it and what blocking is available now.

The analysis

The dossier read back as it stood at 13 Oct 2026, 22:03: where the evidence disagrees with the account given, what the risk looks like, and what remained unanswered. Advisory throughout — it proposes questions and never alters the evidence.

Where the evidence disagrees with the account

CONTRADICTION 1 OF 3 · 90% CONFIDENCE · EVIDENCE CFAD5219	
STATED	The server has not been patched since install and is vulnerable to ProxyLogon (CVE-2021-26855).
THE EVIDENCE SHOWS	AdminDisplayVersion and ExSetup.exe both report 15.2.1544.4. That build is Exchange 2019 CU14, released February 2024 — years after ProxyLogon was patched (KB5000871, March 2021). A server at this build is not vulnerable to CVE-2021-26855.
WHAT WOULD SETTLE IT	Confirm the CU and list installed SUs (Get-ExchangeServer fl AdminDisplayVersion plus Add/Remove Programs "Security Update for Exchange" entries), and check C:\ExchangeSetupLogs for the upgrade history. Then drop the ProxyLogon hypothesis unless an SU regression is shown.

CONTRADICTION 2 OF 3 · 85% CONFIDENCE · EVIDENCE AF0598EA	
STATED	The avenue of attack is a software vulnerability.
THE EVIDENCE SHOWS	The IIS log shows ~1,400 401s across 41 usernames from a /24, followed by clean 200s on g.mertens from a single IP in the same /24. No 500s, no ProxyLogon-style /owa/auth/*.js or SSRF-shaped URIs. That is the signature of a password-spray/credential-stuffing hit landing on one account — not exploitation of a server bug.
WHAT WOULD SETTLE IT	Correlate against the EWS basic-auth MFA exclusion membership and the GM's admitted password reuse with the warehouse portal. If g.mertens is in the exclusion and the warehouse credential was reusable, the vulnerability avenue should be reclassified as credential compromise + authentication weakness.

CONTRADICTION 3 OF 3 · 60% CONFIDENCE	
STATED	Assume full mailbox compromise until shown otherwise.
THE EVIDENCE SHOWS	Reasonable as a working posture, but no mailbox audit log, MailItemsAccessed data, or rule/forwarder enumeration has been collected yet, so "full compromise" is currently an assumption, not a finding.
WHAT WOULD SETTLE IT	Pull Search-MailboxAuditLog and UAL for g.mertens for 3–6 Oct, enumerate inbox rules, transport rules, and SMTP forwarders, and check for any OAuth app consents.

The risk picture

WHAT WAS EXPOSED	On-prem Exchange 2019 published directly to the internet with EWS and IMAP still accepting basic authentication under an MFA-policy exclusion that was added for a scanner in 2023 and never removed.
HOW FAR IT REACHED	Confirmed interactive EWS access to the GM's mailbox from 03 Oct 02:14 onwards. Lateral reach via reused password is plausible (warehouse portal admitted). Scope to other mailboxes unknown — depends on whether any other account in the exclusion returned 200.
DATA PLAUSIBLY TOUCHED	CUSTOMER PERSONAL DATA COMMERCIAL/CONTRACTUAL CORRESPONDENCE CREDENTIALS POTENTIALLY PRESENT IN MAIL BODIES
CONFIDENCE	55%

Notifiability — an opinion, not a determination

Opinion: this looks notifiable. A single external actor obtained authenticated mailbox access to an executive mailbox that the operator believes contained customer personal data, and containment is not yet confirmed. Under GDPR Art. 33 the 72-hour clock arguably started on 6 Oct when the GM reported it; that window has already closed. Final call depends on what the mailbox actually held and whether exfiltration can be ruled out from the audit log.

WHAT WOULD MOST CHANGE THIS

- mailbox audit log contents for g.mertens
- presence of new inbox rules or forwarders
- whether other accounts also returned 200 from the attacker range
- actual data categories and volumes in the GM mailbox
- whether anything has been contained since 6 Oct

Questions raised and added to the questionnaire

PRIORITY	QUESTION
HIGH	Build 15.2.1544.4 corresponds to Exchange 2019 CU14 (released Feb 2024). Confirm the CU level and the last SU applied — this is well after ProxyLogon was patched. The operator believes the server is unpatched since install; the build says otherwise. This changes the whole theory of the case.
HIGH	What does Search-MailboxAuditLog for g.mertens show for 3–6 Oct — MailItemsAccessed, Send, Move, rule changes? Determines what the attacker actually did inside the mailbox after the 200 responses.
HIGH	Any new inbox rules, transport rules, or SMTP forwarders on g.mertens or tenant-wide since 3 Oct? Standard persistence after a mailbox takeover; also drives the "replies to emails he never sent" symptom.
HIGH	List the accounts in the EWS/IMAP basic-auth MFA exclusion. Is g.mertens on it? If the GM is in the exclusion, credential stuffing over EWS basic auth fully explains the 200s without any CVE.
HIGH	Has the warehouse portal had a known breach, and when was the GM's password last changed there before 3 Oct? The GM admits password reuse; a prior leak on the other side is the most likely credential source.

HIGH	For 203.0.113.0/24 and 203.0.113.51, which other usernames ever returned 200 between 1 Oct and now? Scopes blast radius beyond the GM.
HIGH	Since 6 Oct, what has been done — password reset, token/session revoke, basic auth disabled on EWS/IMAP, exclusion removed, IP block, mailbox rules purged? Operator says "not contained". Need the actual state.
HIGH	What is actually in the GM's mailbox — customer PII volumes, contracts, cleartext credentials? Drives notifiability and customer-notice scope.
HIGH	Who outside the business has been told so far — regulator, insurer, customers, MSP in writing? Clock-driven obligations may already be running.
MEDIUM	Is there a WAF, reverse proxy, or geo-filter in front of MAIL01? Affects both the attack path and future containment options.
MEDIUM	What do C:\ExchangeSetupLogs show for install and last upgrade dates on MAIL01? Resolves the contradiction between "never patched" and the CU14-era build.
LOW	What is known about 203.0.113.0/24 and 203.0.113.51 — ASN, geolocation, prior sightings? Supports attribution and block decisions.

Appendix A — The questionnaire

Every question that applied to this incident, with the answer standing at the time of generation. Unanswered questions are listed too: a gap at the time is part of what this report rests on.

QUESTION	ANSWER
How did we first notice?	A person reported it
When was it first noticed?	2026-10-06
Which systems are known to be involved?	MAIL01 (on-prem Exchange). The GM's mailbox for certain. Unclear whether others.
What kind of data could have been reached?	Customer personal data, Commercial or contractual, Credentials
Does the attacker still have access?	Believed not, not confirmed
Has anyone outside the business been told yet?	Not answered
Which product?	Microsoft Exchange Server
Which EXACT version or build?	2019
Where did that version come from?	From memory
Was it reachable from the internet?	Yes, directly
Is a CVE or vendor advisory known?	CVE-2021-26855 — ProxyLogon, we think
Was a patch available when this happened?	Yes
How long had the patch been out?	Years. I do not believe it has been patched since it went in.
Was anything in front of it?	Not answered
What SUs are listed in Add/Remove Programs on MAIL01, and what does the HotFixes list under Get-ExchangeServer fl * show?	Not answered RAISED BY THE ANALYSIS
What do C:\ExchangeSetupLogs show for install and last upgrade dates on MAIL01?	Not answered RAISED BY THE ANALYSIS
For the attacker /24 and 203.0.113.51, which usernames returned 200 at any point between 1 Oct and now?	Not answered RAISED BY THE ANALYSIS
What does the mailbox audit log for g.mertens show for 3–6 Oct — items sent, rules created, folder permissions changed, forwarding set?	Not answered RAISED BY THE ANALYSIS

Are there any new inbox rules, transport rules, or SMTP forwarders on the GM's mailbox or tenant-wide?	Not answered
RAISED BY THE ANALYSIS	
Which accounts are in the MFA exclusion for EWS/IMAP, and is g.mertens one of them?	Not answered
RAISED BY THE ANALYSIS	
Where else was that password used, and have all of those been rotated?	Not answered
RAISED BY THE ANALYSIS	
What is actually in the GM's mailbox — customer PII volumes, contracts, cleartext credentials?	Not answered
RAISED BY THE ANALYSIS	
What has actually been done since 6 Oct — password reset, token revoke, basic auth disabled. MFA exclusion removed, IP blocks?	Not answered
RAISED BY THE ANALYSIS	
Who outside the business has been told so far — regulator, insurer, customers, MSP in writing?	Not answered
RAISED BY THE ANALYSIS	
Is there a WAF, reverse proxy, or geo-filter in front of MAIL01?	Not answered
RAISED BY THE ANALYSIS	
What is known about 203.0.113.0/24 and 203.0.113.51 — ASN, geolocation, prior sightings?	Not answered
RAISED BY THE ANALYSIS	
Build 15.2.1544.4 corresponds to Exchange 2019 CU14 (released Feb 2024). Confirm the CU level and the last SU applied — this is well after ProxyLogon was patched.	Not answered
RAISED BY THE ANALYSIS	
What does Search-MailboxAuditLog for g.mertens show for 3–6 Oct — MailItemsAccessed. Send, Move, rule changes?	Not answered
RAISED BY THE ANALYSIS	
Any new inbox rules, transport rules, or SMTP forwarders on g.mertens or tenant-wide since 3 Oct?	Not answered
RAISED BY THE ANALYSIS	
List the accounts in the EWS/IMAP basic-auth MFA exclusion. Is g.mertens on it?	Not answered
RAISED BY THE ANALYSIS	
Has the warehouse portal had a known breach, and when was the GM's password last changed there before 3 Oct?	Not answered
RAISED BY THE ANALYSIS	
For 203.0.113.0/24 and 203.0.113.51, which other usernames ever returned 200 between 1 Oct and now?	Not answered
RAISED BY THE ANALYSIS	

Since 6 Oct, what has been done — password reset,
token/session revoke, basic auth disabled on EWS/IMAP,
exclusion removed, IP block, mailbox rules purged?

Not answered

RAISED BY THE ANALYSIS

Appendix B — The dossier

Everything ever recorded against this incident, newest first, including what was later corrected or withdrawn. Withdrawn material is shown rather than removed: a dossier that silently drops what it no longer believes cannot be checked.

13 OCT 2026, 22:37 · LOG FILE · 95% CONFIDENCE

STANDING

Raw IIS log, MAIL01, 3 Oct (attached)

The file itself rather than a paste.

Attachment on the record: u_ex_iis_20261003.log

Reference 86e3420c-1c1b-4afe-811a-99041ca92819

13 OCT 2026, 21:50 · LOG FILE · 95% CONFIDENCE

STANDING

Get-ExchangeServer output, MAIL01, taken 6 Oct

Pulled by the MSP while we were on the phone.

```
[PS] C:\> Get-ExchangeServer MAIL01 | fl Name,Edition,AdminDisplayVersion

Name                : MAIL01
Edition              : Standard
AdminDisplayVersion  : Version 15.2 (Build 1544.4)

[PS] C:\> Get-Command ExSetup.exe | ForEach {$_.FileVersionInfo}
ProductVersion  FileVersion  FileName
-----
15.02.1544.004  15.02.1544.004  C:\Program Files\Microsoft\Exchange Server\V15\bin\ExSetup.exe
```

Reference cfad5219-a159-46ef-b220-9d1ffffa894f

13 OCT 2026, 21:50 · LOG FILE · 90% CONFIDENCE

STANDING

IIS log extract, MAIL01, 2-3 Oct

g.mertens is the GM. No 500s and no /owa/auth/x.js style requests anywhere in the window.

```
# Fields: date time cs-method cs-uri-stem c-ip cs-username sc-status
2026-10-02 21:04:11 POST /EWS/Exchange.asmx 203.0.113.44 j.okafor 401
2026-10-02 21:04:12 POST /EWS/Exchange.asmx 203.0.113.44 l.hargreaves 401
2026-10-02 21:04:14 POST /EWS/Exchange.asmx 203.0.113.44 d.whitlam 401
... 1,418 further 401 responses, 41 distinct usernames, same /24 ...
2026-10-03 02:14:52 POST /EWS/Exchange.asmx 203.0.113.51 g.mertens 200
2026-10-03 02:15:03 POST /EWS/Exchange.asmx 203.0.113.51 g.mertens 200
2026-10-03 02:19:40 POST /EWS/Exchange.asmx 203.0.113.51 g.mertens 200
2026-10-03 06:51:18 POST /EWS/Exchange.asmx 203.0.113.51 g.mertens 200
```

Reference af0598ea-3454-4bce-8179-6fbe0550bcf8

13 OCT 2026, 21:50 · SYSTEM DETAIL · 85% CONFIDENCE

STANDING

Authentication posture on MAIL01

Confirmed in the portal, not from memory.

OWA and ActiveSync sit behind the tenant MFA policy. EWS and IMAP still accept basic authentication – exclusion added in 2023 for the stocktake scanner and never removed. Conditional access does not cover the exclusion.

Reference 7da6ecf6-2d9b-45fb-8cbc-2747d220e688

Statement — GM

Password was the same one I use for the warehouse portal. I know. I have changed both.

Reference 7221a8d9-43ca-43b8-b904-4573dc6d5db2

The full exchange with the model is held on the record and can be included in this document on request.