

Vantalect

AWS INCIDENT RESPONSE · SAMPLE DELIVERABLE

Operational Situation Reports

DISTRIBUTION: OPERATIONAL

Days 1 to 6: the fixed rhythm · prepared for Wrenfield Bancorp, Inc.

Prepared by Charles Sieg · charles.sieg@vantalect.com · vantalect.com

July 9, 2026 · AWS Incident Response: The Response (July 4 to 9, 2026)

SAMPLE DELIVERABLE

This is a sample deliverable. Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

Contents

What these reports are, and what they are not **3**

The reports at a glance **4**

Stage 0 Activation: the bridge opens **6**

SR-01: Saturday, July 4, 01:00 EDT (05:00 UTC) 6

Stage 1 Stop the bleeding: contain, and close the outside door **8**

SR-02: Saturday, July 4, 02:00 EDT (06:00 UTC) 9

SR-03: Saturday, July 4, 03:00 EDT (07:00 UTC) 11

SR-04: Saturday, July 4, 04:00 EDT (08:00 UTC) 13

SR-05: Saturday, July 4, 05:00 EDT (09:00 UTC) 15

Stage 2 Preserve: evidence kept, deleted snapshots back **17**

SR-06: Saturday, July 4, 09:30 EDT (13:30 UTC) 17

SR-07: Saturday, July 4, 21:30 EDT (July 5, 01:30 UTC) 18

Stage 3 Protect and recover: rewrite the archive, fill the vault **20**

SR-08: Sunday, July 5, 09:30 EDT (13:30 UTC) 20

SR-09: Sunday, July 5, 21:30 EDT (July 6, 01:30 UTC) 21

SR-10: Monday, July 6, 09:30 EDT (13:30 UTC) 23

SR-11: Monday, July 6, 21:30 EDT (July 7, 01:30 UTC) 24

Stage 4 Eradicate: the deadline passes, the attacker's identities go **26**

SR-12: Tuesday, July 7, 09:30 EDT (13:30 UTC) 26

SR-13: Tuesday, July 7, 21:30 EDT (July 8, 01:30 UTC) 27

SR-14: Wednesday, July 8, 09:30 EDT (13:30 UTC) 29

SR-15: Wednesday, July 8, 21:30 EDT (July 9, 01:30 UTC) 30

Stage 5 Containment declared **32**

SR-16: Thursday, July 9, 09:30 EDT (13:30 UTC) 32

Notice **33**

Distribution

This report is for the bank's incident and platform teams. It is not part of the counsel track and holds no legal analysis.

What these reports are, and what they are not

These are the 16 situation reports of the Response, compiled on Thursday, July 9, 2026, and each one states only what we knew at its own time. We did not rewrite an earlier report with hindsight. Where a later report corrects an earlier one, it says so in its own text.

Who receives them. These are operational reports for the bank's incident team, the people that outside counsel, Diane Whitcombe of Tessaly & Brook LLP, names. Counsel keeps the list and decides what goes beyond it, to regulators, the insurer, or anyone else. They hold facts, actions, decisions, owners, and deadlines for approvers.

What the reports do not do. They hold no legal analysis and make no legal determination. Where a report once carried a legal question, it carries one line pointing to the counsel notes in the clock worksheet (Report 4) instead. Each action's approver, evidence, and rollback are in the action register (the containment report), and the evidence is in the custody log. None of that is repeated here. The root causes and the full attack narrative belong to the Investigation.

How to read one report. Every report has the same eight parts in the same order, so a reader can go straight to the part they need.

The eight parts of every situation report, in the order they appear.

Part	What it holds
Headline	The one sentence that matters now
Confirmed	Facts we have read in a log or seen in a console, with the time
Working hypotheses	What we think, labeled as not confirmed
Actions since the last report	What was done, by whom, at what time
Proposed, awaiting approval	What we recommend and have not yet done
Decisions needed	What someone must decide, who owns it, and by when
Deadlines running	Operational deadlines that were running at that moment
Not yet known	What we could not yet say

Times are Eastern Daylight Time (EDT, UTC−4), with UTC beside the report's own time. Attacker addresses are from ranges reserved for documentation. Consultant effort is stated only as a total.

The reports at a glance

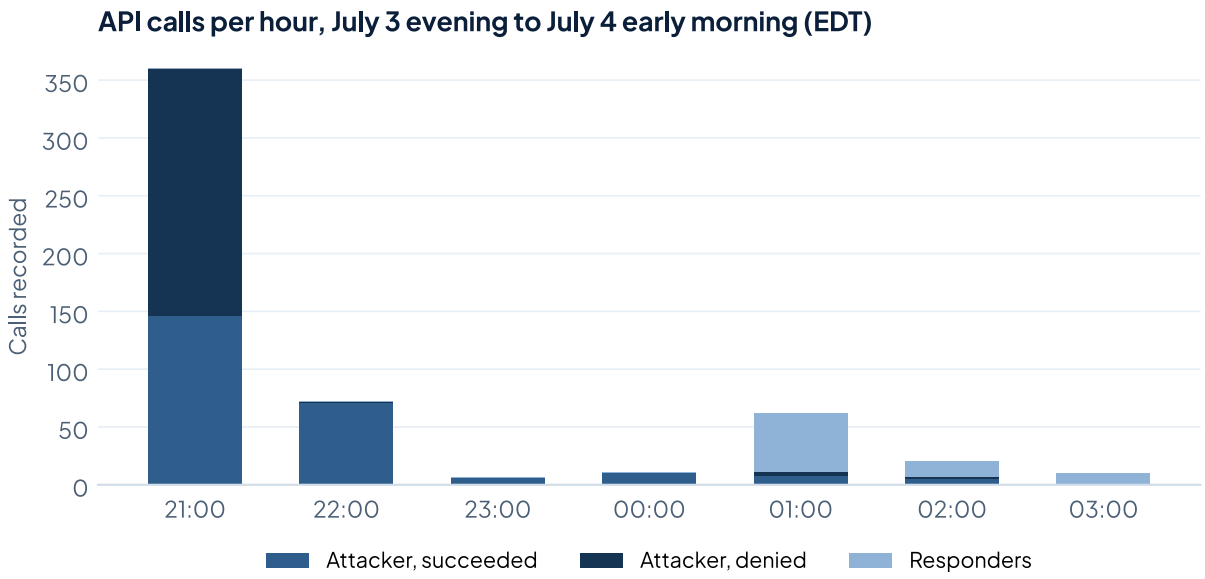
The rhythm was hourly while the attacker was still active and the containment was being built, then every 12 hours. 37 attacker sessions ran in the workload accounts, and the destructive work was done in about two and a half hours on Friday night. After the containment policy attached at 01:22 EDT, the attacker's calls fell to single digits an hour, and the last was at 03:00 on Saturday. The bank's trail holds nothing from the attacker after that. The figure shows the hours around it. Stage names follow the Response page, from Stage 0 Activation to Stage 5 Containment declared.

Situation reports 1 to 8: stage 0 (activation), stage 1 (hourly), stage 2, and the start of stage 3.

Report	As of (EDT)	UTC	Stage	Headline
SR-01	Sat, July 4, 01:00 EDT	05:00 UTC	0	The attacker has locked data and demanded payment. We are on the bridge with no access of our own, and containment is drafted but not applied.
SR-02	Sat, July 4, 02:00 EDT	06:00 UTC	1	Containment is on and the deploy-role path is cut, but denied calls show the attacker holds other credentials. The loan snapshot is still shared with the outside account.
SR-03	Sat, July 4, 03:00 EDT	07:00 UTC	1	The share and the outside key statements are removed, a second key was in use until 02:50, persistence is mapped and denied, and the copy-out is probable.
SR-04	Sat, July 4, 04:00 EDT	08:00 UTC	1	Persistence is shut, the outside door is closed by policy, and evidence is going into a locked account. The attacker has been silent for an hour.
SR-05	Sat, July 4, 05:00 EDT	09:00 UTC	1	Stage 1 is complete. The vault exists, and the first use of the stolen key is traced to the Monday before.
SR-06	Sat, July 4, 09:30 EDT	13:30 UTC	2	Quiet for six and a half hours. Deleted snapshots are back, the FBI has the first call, and the bank's leadership meets with counsel at 10:00.
SR-07	Sat, July 4, 21:30 EDT	July 5, 01:30 UTC	2	The FBI has the complaint. No host access found; the archive reads cannot be known.
SR-08	Sun, July 5, 09:30 EDT	13:30 UTC	3	The month-end snapshots are back and the bank's own rewrite of the archive has started, in sequential slices.

Situation reports 9 to 16: the rest of stage 3, stage 4, and stage 5. Each stage heading below names its rhythm.

Report	As of (EDT)	UTC	Stage	Headline
SR-09	Sun, July 5, 21:30 EDT	July 6, 01:30 UTC	3	The vault is being filled and the rewrite is on pace. The bank's trail shows nothing from the attacker since Saturday, and it could not show a denied try on the lending key.
SR-10	Mon, July 6, 09:30 EDT	13:30 UTC	3	The rewrite is about halfway and the vault copies are most of the way done. The volume snapshot copies are locked. No attacker call since Sunday afternoon.
SR-11	Mon, July 6, 21:30 EDT	July 7, 01:30 UTC	3	The vault copies are complete, the live-database recovery point is locked, and the database copies rest on policy. Tuesday is the attacker's deadline.
SR-12	Tue, July 7, 09:30 EDT	13:30 UTC	4	The rewrite is nearly done with hours to spare before the keys expire.
SR-13	Tue, July 7, 21:30 EDT	July 8, 01:30 UTC	4	The deadline has passed. The bank reports that its 14:00 check found no current object under the attacker's keys, and nothing was paid.
SR-14	Wed, July 8, 09:30 EDT	13:30 UTC	4	Eradication is ready to start in half an hour, after preservation.
SR-15	Wed, July 8, 21:30 EDT	July 9, 01:30 UTC	4	The attacker's identities are gone, the deploy role is narrowed, and loan origination is back online. The attacker's keys stay in PendingImport; the calls to disable them were rejected.
SR-16	Thu, July 9, 09:30 EDT	13:30 UTC	5	Containment is declared in writing. This is the last report of the Response.



API calls recorded per hour in the organization trail, Friday evening to Saturday morning, EDT: the attacker's allowed calls, the attacker's denied calls, and the responders' calls.

Stage 0 Activation: the bridge opens

One report, Saturday, July 4, at 01:00 EDT. Written two minutes after we joined the bridge, from the bank's screens, before we had access of our own.

SR-01: Saturday, July 4, 01:00 EDT (05:00 UTC)

As of: Saturday, July 4, 01:00 EDT (05:00 UTC). **Stage:** Stage 0 Activation: the bridge opens. **Report:** 1 of 16.

Headline. The attacker has locked data and demanded payment. We are on the bridge with no access of our own, and containment is drafted but not applied.

Where these facts come from. We have no access of our own yet. Everything below is from the bank's screens shared on the bridge and from Imani Castell and Owen Tribble reading the organization trail.

Confirmed.

- A ransom note, `RESTORE-INSTRUCTIONS.txt`, was found in 3 buckets (imaging, data lake, and lending), written at 23:30 Friday. The trail holds 2 of the writes, and the third bucket has no data events, so that copy was seen in a listing. The note demands $14,500,000 in cryptocurrency by Tuesday, July 7, 18:00 EDT. The contact in the note is withheld from this set.
- GuardDuty raised a finding at 22:44 EDT, and the managed provider paged Owen Tribble at 23:18 EDT, 34 minutes later. Owen Tribble confirmed the note at 00:05.
- The trail shows sessions of the role `wf-deploy-pipeline` from `203.0.113.47` in the workload accounts. The first write-capable one began at 21:04 EDT Friday, 3 hours 56 minutes before this report. The caller is the IAM user `svc-artifact-sync` in `wf-tools`, using the access key `AKIAWRFNEXAMPLE00001`.
- Three KMS keys with the alias `alias/wf-backup-2026` were created at 21:06 and 21:09 in the lending, imaging, and data production accounts, each with key material imported from outside AWS.
- An S3 Batch Operations job in the imaging account has been copying objects since 21:41, and it is still running.
- At 00:47 deletion protection was turned off on the loan database `wf-los-prod`.
- The bank's 9 month-end database snapshots and its 46 volume snapshots in the production accounts were deleted Friday night, at 22:05 and 22:09.
- A database snapshot copy was shared with the account `777788889999` at 23:51 EDT. The account is not one of the bank's 20.

Working hypotheses (not confirmed).

- The attacker was active at 00:47 and should be treated as still inside.
- Turning off deletion protection on `wf-los-prod` is preparation to delete it.
- The shared snapshot may have been copied into the other account. We have no evidence yet either way.
- The deploy role and key 1 are not necessarily the whole path in. We do not yet know what else was created.

Actions since the last report. This is the first report. Before the bridge: Owen Tribble called Imani Castell and Mireille Danvers at 00:05, Mireille Danvers called Harold Penwick at 00:20, Harold Penwick called Diane Whitcombe at 00:34. Diane Whitcombe called us at 00:41. The incident statement of work was signed at 00:52 EDT. Charles Sieg joined the bridge at 00:58.

Proposed, awaiting approval.

- A containment policy on the Workloads OU, drafted from our template and being edited by Imani Castell. It would deny key-origin and imported-material changes, snapshot deletion and sharing, database deletion and modification, lifecycle, versioning, and trail changes, new IAM users, keys, and roles, and S3 Batch job creation, for every principal except the incident role and the bank's break-glass role.
- Deactivate the key `AKIAWRFNEXAMPLE00001`, then revoke the deploy role's active sessions in the ten workload accounts, then cancel the S3 Batch job.
- Deploy our incident role to every account by StackSet so we can read for ourselves.

Decisions needed.

- Approve the containment policy. Owner: Mireille Danvers. By 01:20 EDT.
- Notify the broker's claims hotline. Owner: Harold Penwick. By 01:15 EDT.
- Take loan origination offline to freeze its state, or leave it running. Owner: Rafael Quintero, with Lucía Brandt. By 02:00 EDT.

Deadlines running.

- The attacker's deadline in the note: Tuesday, July 7, 18:00 EDT (22:00 UTC), 3 days 17 hours from now.
- The bank's volume-snapshot Recycle Bin rule keeps deleted snapshots for ten days. Whether the deleted snapshots landed there has not been checked.

Not yet known. How many objects the S3 Batch job has changed. When the imported key material expires. How the attacker got the key. What else the attacker created. Whether data left the organization. Whether the loan database is intact.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

Stage 1 Stop the bleeding: contain, and close the outside door

Hourly, Saturday, July 4, 02:00 to 05:00 EDT. From the containment policy until the exfiltration path, the outside door, and the recovery vault were settled.

SR-02: Saturday, July 4, 02:00 EDT (06:00 UTC)

As of: Saturday, July 4, 02:00 EDT (06:00 UTC). **Stage:** Stage 1 Stop the bleeding: contain, and close the outside door. **Report:** 2 of 16.

Headline. Containment is on and the deploy-role path is cut, but denied calls show the attacker holds other credentials. The loan snapshot is still shared with the outside account.

Confirmed.

- The S3 Batch job was canceled at 01:28 after 3 hours 47 minutes. At the cancel, 61.3 million of the archive's 286 million objects (21.4%) have an attacker-key current version. The bank-key versions are now noncurrent but intact, because versioning is on.
- All three attacker keys were imported with an expiry of Tuesday, July 7, 18:00 EDT, the same moment as the ransom deadline. Each key's policy is the account default plus a statement for the account `777788889999`.
- **The loan snapshot copy is still shared with the outside account, and the three key policies still name it.** The share has been open 2 hours 8 minutes as of this report. The containment policy blocks new changes in the workload accounts. It does not remove a share or a key statement that already exists.
- Friday at 21:12 EDT, the attacker tried to re-encrypt data-lake objects with customer-supplied keys (SSE-C). All 214 calls were denied in 40 seconds. No data-lake object was encrypted that way.
- The attacker put a lifecycle rule on the imaging archive at 21:14 to expire noncurrent versions after one day. It would have begun deleting the bank-key versions, the only copies not under attacker keys. We removed it at 01:35.
- The trail shows an IAM user `aws-support-sync` created at 22:31 with an administrator policy and an access key, and a role `OrgAccessBackup` created at 22:36 that trusts the account `777788889999`.
- Three calls after the containment policy were denied: at 01:24 a deploy-role session's `CreateAccessKey` for `aws-support-sync` (`EV-00544`), at 01:31 `DeleteImportedKeyMaterial` on the data-lake key, made by `aws-support-sync` in `wf-prod-data`, the key's own account (`EV-00566`), and at 01:39 `DeleteDBInstance` on `wf-los-prod` (`EV-00570`). The last two did not come from the deploy role.
- Our incident role reached all 20 accounts at 01:40, 42 minutes after we joined the bridge. Our first reads ran from 01:44 in six accounts.
- The bank took loan origination offline at 01:50.

- The organization trail is unbroken. The attacker deleted a legacy trail in the lending account at 22:14, then tried to stop the organization trail at 22:15 and was denied.

Working hypotheses (not confirmed).

- The attacker holds at least one credential besides key 1: the user `aws-support-sync`, the role `OrgAccessBackup`, or both. The two denied calls that did not come from the deploy role point there.
- The shared snapshot probably was copied into the outside account. Calls from that account on the lending key appear in the bank's log from 00:06, and we are counting and classifying them.
- While the share and the key statements stand, the attacker could retry or finish an incomplete copy at will.
- Until the imported material expires, the keys work and the bank can read what the attacker re-encrypted. If so, the bank can rewrite it under its own keys before the deadline.

Actions since the last report.

- 01:15, the broker's claims hotline notified (bank).
- 01:16 and 01:22, the containment policy created and attached to the Workloads OU. Mireille Danvers approved, Imani Castell attached it.
- 01:24, the key `AKIAWRFNEXAMPLE00001` set to Inactive.
- 01:26, active sessions revoked on `wf-deploy-pipeline` in the ten workload accounts.
- 01:28, the S3 Batch job canceled.
- 01:35, the attacker's lifecycle rule removed.
- 01:31:40, a self-managed StackSet created in the management account. CloudFormation assumes the bank's break-glass role in each member account, which the containment policy exempts. By 01:40:09 the incident role existed in the other 19 accounts. Imani Castell created the management account's copy separately, by a stack at 01:40:25 and a role at 01:40:31.
- 01:50, loan origination taken offline by the bank.

Proposed, awaiting approval.

- **Capture, then close the exfiltration path.** First record the snapshot's sharing attributes, the three attacker key policies, and the three key grant lists into the custody log. Then remove the outside account from the snapshot's restore attribute, drop the outside statement from the three key policies, and revoke the attacker's grant. The bank's break-glass role does the changes, because the containment policy exempts it.
- Stand up Pursuit in `wf-audit`, seeded with key 1, to follow every session the key and the deploy role opened.

- When Pursuit's list of what the attacker created is complete, deny everything for those identities in one change to the containment policy, and deactivate any second key.

Decisions needed.

- Approve the capture and the closure of the exfiltration path. Owner: Mireille Danvers. By 02:05 EDT.
- Approve Pursuit in `wf-audit`. Owner: Mireille Danvers. By 02:15 EDT.
- Tell the chief executive. Owner: Harold Penwick, with Mireille Danvers. By 07:00 EDT.
- The insurer's written consent is awaited. Owner: Harold Penwick, through the broker.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 3 days 16 hours from now.
- The Recycle Bin check is still open.

Not yet known. Whether data was copied out. Whether a second access key exists and is in use. What else the attacker created. Whether the nonproduction and sandbox accounts were touched beyond reads. Whether the deleted snapshots are recoverable.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

SR-03: Saturday, July 4, 03:00 EDT (07:00 UTC)

As of: Saturday, July 4, 03:00 EDT (07:00 UTC). **Stage:** Stage 1 Stop the bleeding: contain, and close the outside door. **Report:** 3 of 16.

Headline. The share and the outside key statements are removed, a second key was in use until 02:50, persistence is mapped and denied, and the copy-out is probable.

Confirmed.

- **The exfiltration path is closed.** At 02:03 to 02:05 we captured the snapshot's sharing attributes (`EV-00625`), the three key policies (`EV-00626` to `EV-00628`), and the three grant lists (`EV-00629` to `EV-00631`) into the custody log. At 02:08:20 EDT Imani Castell removed `777788889999` from the snapshot's restore attribute (`EV-00632`), after the share had been open 137 minutes. At 02:09 three `PutKeyPolicy` calls dropped the outside statement from the three attacker keys (`EV-00633` to `EV-00635`). At 02:10:30 EDT the attacker's grant was revoked (`EV-00636`). The bank's break-glass role made all five changes.

- **A second door was open as well.** At 01:36, a session from the account `777788889999` assumed `OrgAccessBackup` in the lending account (`EV-00569`). The assumption succeeded and gave an administrator session, `S-0040`, for one hour. A service control policy cannot stop a principal outside the organization from assuming a role that trusts it. The policy blocked only what followed, the `DeleteDBInstance` at 01:39.
- Pursuit went live in `wf-audit` at 02:20. It follows the 37 sessions of `wf-deploy-pipeline`, which the trail shows in 10 accounts, and finds one user, one access key, and two roles created: `aws-support-sync`, `AKIAWRFNEXAMPLE00002`, `OrgAccessBackup`, and `s3-batch-replication`.
- At 02:47 to 02:50, the second key `AKIAWRFNEXAMPLE00002` was used from `203.0.113.47` for `GetCallerIdentity`, `ListAccessKeys`, `ListBuckets`, `GetSessionToken`, and `DescribeDBInstances` (`EV-00637` to `EV-00641`). They are read-only calls that the containment policy does not deny. Pursuit alerted at 02:50.
- At 02:58 the containment policy was updated to deny everything for `aws-support-sync`, `OrgAccessBackup`, and `s3-batch-replication`. The attacker's first call afterward, at 02:59, was denied.
- Between 00:06:09 EDT and 00:51:06 EDT, principals in the account `777788889999` made 7 KMS calls on the attacker's lending key, logged in the bank's account: 2 `CreateGrant` (one for the outside role `exfil-runner`, one for RDS with that role as the retiring principal), 1 `DescribeKey`, 1 `ReEncrypt` to a key in the outside account, 2 `Decrypt`, and 1 `RetireGrant`. That is the pattern of a snapshot copy into another account. **We assess the copy-out as probable, with high confidence.** It is not confirmed, because the other account's logs are not ours.
- The snapshot belongs to the loan origination database `wf-los-prod`. What data it holds, and how many people, is for the bank to establish.
- The 46 deleted volume snapshots are in the Recycle Bin. The 9 deleted month-end database snapshots have intact copies in `wf-backup`.

Working hypotheses (not confirmed).

- The attacker will retry through whatever remains. The second key and the outside role are the open ends.
- The set of persistence we have found may be incomplete. Only a full sweep, later, can say.
- The closure stops a new copy of this snapshot. It does not recall a copy already made.

Actions since the last report.

- 02:03 to 02:05, the share, key policies, and grants captured (we did, through the incident role).
- 02:08:20 to 02:10:30, the share removed, the three key policies rewritten, and the grant revoked (Imani Castell, break-glass role).

- 02:10, the insurer's written consent arrived.
- 02:20, Pursuit live in `wf-audit`.
- 02:50, Pursuit alert on the second key.
- 02:58, the containment policy updated (Mireille Danvers approved, Imani Castell applied).

Proposed, awaiting approval.

- Deactivate `AKIAWRFNEXAMPLE00002`. Mireille Danvers has approved it, and Imani Castell is applying it as this report issues.
- A resource control policy on the Workloads OU that denies calls from outside the organization: `sts:AssumeRole` and its companions, all KMS actions, and all S3 actions. AWS services are exempt, and one named responder principal is exempt for the role assumption.
- A new OU named Incident, with an account `wf-ir-forensics` that holds only evidence, and a bucket in it with Object Lock.

Decisions needed.

- Approve the resource control policy. Owner: Mireille Danvers. By 03:15 EDT.
- Approve the Incident OU and the evidence account. Owner: Mireille Danvers. By 03:10 EDT.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 3 days 15 hours from now.
- The Recycle Bin keeps the deleted volume snapshots for ten days from deletion, to about July 13.

Not yet known. When the key was first used. Whether anything was read from the imaging archive (reads on that bucket are not logged; only writes are). What data the shared snapshot holds. Whether the outside account can still use the attacker's keys on other resources.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

SR-04: Saturday, July 4, 04:00 EDT (08:00 UTC)

As of: Saturday, July 4, 04:00 EDT (08:00 UTC). **Stage:** Stage 1 Stop the bleeding: contain, and close the outside door. **Report:** 4 of 16.

Headline. Persistence is shut, the outside door is closed by policy, and evidence is going into a locked account. The attacker has been silent for an hour.

Confirmed.

- The attacker's last call was at 03:00, a denied `ListUsers` (`EV-00644`). We have seen nothing since in the trail.
- The second key was set to Inactive at 03:01.
- The Incident OU was created at 03:11, the account `wf-ir-forensics` (`584729107701`) at 03:12, and the account was moved into the OU at 03:14.
- At 03:15 the resource control policy type was enabled at the organization root (`EV-00650`). At 03:16 an Access Analyzer listing in `wf-audit` (`EV-00652`) read the outside trusts that exist: the attacker's `OrgAccessBackup` trust, still present, and our incident role, which is exempt. The bank had no other outside trust for the policy to cut.
- The resource control policy `wf-deny-outside-access` was created at 03:19 and attached to the Workloads OU at 03:20. Since then no principal outside the organization can assume a role in a workload account, except one named responder principal, and none can make a KMS or S3 call there. AWS services are exempt.
- The bucket `wf-ir-evidence` exists in `wf-ir-forensics` with Object Lock in compliance mode and a seven-year default retention, created at 03:40. Evidence preservation has begun.
- No object in the data lake was encrypted by the attacker. The SSE-C attempts all failed, and the logged writes on that bucket show only the ransom note besides the failed attempts.

Working hypotheses (not confirmed).

- The attacker is waiting rather than gone. A silent hour is not evidence of exit.
- The outside account has no route to the attacker's keys that we know of. The three key policies no longer name it, and the resource control policy denies its KMS calls. A full sweep, later, is what can confirm that.

Actions since the last report.

- 03:01, the second key `AKIAWRFNEXAMPLE00002` deactivated.
- 03:11 to 03:14, the Incident OU and `wf-ir-forensics` created (Mireille Danvers approved, Imani Castell executed).
- 03:15 to 03:20, the policy type enabled, the outside trusts listed, and the resource control policy created and attached (Mireille Danvers approved).
- 03:40 and 03:41, the evidence bucket created and locked.

Proposed, awaiting approval.

- A recovery vault: a new account `wf-recovery-vault` in a new Recovery OU, behind a policy that denies everything except two copy roles and the account's default setup role, and that also denies deletion and key changes to everyone. It would hold three vault keys whose origin is AWS KMS, which only the bank holds.
- Restore the 46 deleted volume snapshots from the Recycle Bin at about 07:40, once the deletion events are preserved.
- Tell the FBI field office at about 06:00.

Decisions needed.

- Approve the recovery vault and its policy. Owner: Mireille Danvers, with Rafael Quintero. By 04:30 EDT.
- Call the FBI field office. Owner: Harold Penwick. By 06:00 EDT.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 3 days 14 hours from now.
- The Recycle Bin window, to about July 13.

Not yet known. The first date the key was used. Whether the outside account holds any other access. The size of the data in the shared snapshot. Whether any other account holds attacker-created resources.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

SR-05: Saturday, July 4, 05:00 EDT (09:00 UTC)

As of: Saturday, July 4, 05:00 EDT (09:00 UTC). **Stage:** Stage 1 Stop the bleeding: contain, and close the outside door. **Report:** 5 of 16.

Headline. Stage 1 is complete. The vault exists, and the first use of the stolen key is traced to the Monday before.

Confirmed.

- The Recovery OU was created at 04:29 and the account `wf-recovery-vault` (`584729107714`) at 04:30. The policy `wf-vault-deny-all` was attached to the OU at 04:34. At 04:40 three vault keys with origin AWS KMS were created in the vault account, and the bank holds them.

- The trail traces the key back: **the first use of `AKIAWRFNEXAMPLE00001` was Monday, June 29, 03:14 EDT**, a `GetCallerIdentity` from `198.51.100.23`. The first write-capable session was Friday, July 3, 21:04 EDT. That is a dwell of 4 days, 17 hours, 50 minutes before the first write-capable session, and 4 hours 18 minutes from that session to the containment policy.
- From June 29 to July 2 the attacker worked read-only, each day from about 02:00 to 11:00 EDT: listing roles, keys, buckets, and databases, and reading the deploy role's trust policy. A call to `ListAccounts` was denied. On July 1 the attacker assumed the deploy role once into `wf-nonprod-data`, to test it.
- Those read-only calls reached the organization trail but no alert, so no one was told during the discovery week. The first alert was the GuardDuty finding on July 3.
- The key `AKIAWRFNEXAMPLE00001` was created on March 14, 2023 and never rotated.

Working hypotheses (not confirmed).

- The discovery hours match a single operator working roughly 09:00 to 18:00 in a time zone three hours ahead of UTC. That is a pattern, not an attribution, and we draw no conclusion from it yet.
- The key left the bank's control outside AWS. Nothing in AWS logs says how, and only an interview can.
- The attacker has no foothold inside any host. We have seen only control-plane calls. This is unconfirmed until we have looked at the hosts' logs.

Actions since the last report.

- 04:29 to 04:40, the Recovery OU, the vault account, its deny-all policy, and its three keys (Mireille Danvers approved, Imani Castell executed).
- Evidence preservation continued in `wf-ir-evidence`.

Proposed, awaiting approval.

- Restore the 46 volume snapshots from the Recycle Bin at about 07:40.
- Restore the 9 month-end database snapshots from `wf-backup` on Sunday at 05:10, and copy them, with the live snapshot, into the vault.
- Start a bank-run S3 Batch rewrite on Sunday at 09:00 that copies every noncurrent bank-key version back as current, under a key the bank holds, in 31 sequential slice jobs.
- Move to a report every 12 hours. The next report is at 09:30.

Decisions needed.

- Convene the bank's leadership meeting with counsel for 10:00 EDT. Owner: Harold Penwick, with Diane Whitcombe. By 10:00 EDT.

- Approve the rewrite plan. Owner: Lucía Brandt and Rafael Quintero, who own the workloads. By Saturday 21:30 EDT.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 3 days 13 hours from now.
- The Recycle Bin window, to about July 13.
- The bank's meeting is at 10:00.

Not yet known. Whether the loan platform's hosts were touched. Whether anything was read from the imaging archive. What data the shared snapshot holds. Whether the sweep will find more.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

Stage 2 Preserve: evidence kept, deleted snapshots back

Every 12 hours, Saturday, July 4. Evidence kept safe, deleted snapshots back, the FBI told, and the bank's leadership meeting with counsel.

SR-06: Saturday, July 4, 09:30 EDT (13:30 UTC)

As of: Saturday, July 4, 09:30 EDT (13:30 UTC). **Stage:** Stage 2 Preserve: evidence kept, deleted snapshots back. **Report:** 6 of 16.

Headline. Quiet for six and a half hours. Deleted snapshots are back, the FBI has the first call, and the bank's leadership meets with counsel at 10:00.

Confirmed.

- We have seen no attacker call for six and a half hours, since the denied `ListUsers` at 03:00.
- Loan origination has been offline since 01:50, 7 hours 40 minutes as of this report.
- The 46 volume snapshots are restored. 1 came back in the lending account at 07:40 and 1 in the data account at 07:41.
- The imaging archive is 412 TB in 286 million objects, with versioning on and no Object Lock. That is why the bank-key versions survived.

Working hypotheses (not confirmed).

- The attacker's silence is a pause, not an exit. They may return at the deadline to see whether the bank engages.
- The bank can complete a rewrite of the 61.3 million objects before 18:00 EDT on Tuesday. We have not yet proved the rate.

Actions since the last report.

- 06:00, Harold Penwick reported to the FBI field office.
- 07:40 and 07:41, the 46 volume snapshots restored from the Recycle Bin (Imani Castell).
- The IC3 complaint is being prepared.

Proposed, awaiting approval.

- Sunday 05:10 to Monday, the month-end snapshots restored and copied into the vault.
- Sunday 09:00, the bank's rewrite of the archive in the imaging account.

Decisions needed.

- The bank's leadership meets with counsel at 10:00: Harold Penwick, Mireille Danvers, Anand Sethuraman, and counsel. We attend to supply facts.
- Approve the rewrite plan. Owner: Lucía Brandt and Rafael Quintero. By 21:30 EDT.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 3 days 8 hours 30 minutes from now.

Not yet known. What the meeting decides. Whether the host logs show anything. What data the shared snapshot holds.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

SR-07: Saturday, July 4, 21:30 EDT (July 5, 01:30 UTC)

As of: Saturday, July 4, 21:30 EDT (July 5, 01:30 UTC). **Stage:** Stage 2 Preserve: evidence kept, deleted snapshots back. **Report:** 7 of 16.

Headline. The FBI has the complaint. No host access found; the archive reads cannot be known.

Confirmed.

- The FBI was told at 06:00, and the IC3 complaint was filed at 09:40.

- The bank's leadership met with counsel at 10:00 (Harold Penwick, Mireille Danvers, Anand Sethuraman, and counsel). We attended to supply facts.
- No host access has been found in the Jenkins controller's logs, which were collected at 05:35. The loan platform's logs have not been collected yet. This is a review of the logs the bank has; we state it as what we found, not as proof that none occurred.
- **Reads from the imaging archive cannot be known.** The organization trail logs writes on that bucket, not reads, so an object read by the attacker left no record.
- Loan origination remains offline, 19 hours 40 minutes as of this report.
- No payment has been made. **Working hypotheses (not confirmed).**
- The tools and the infrastructure overlap with a cluster we track as `VTL-C1`, a Vantalect label and not a name. The working hours, and Russian-language artifacts in the note's metadata, are **consistent with a Russian-speaking, financially motivated actor.** It is a hypothesis. We name no group. The indicators go to counsel.

Actions since the last report.

- 09:40, the IC3 complaint filed (bank).
- 10:00, the leadership meeting (bank and counsel).
- Preservation continued: the trail, the policies, and the ransom note copies are in `wf-ir-evidence`.

Proposed, awaiting approval.

- Sunday 05:10, the month-end snapshots restored from `wf-backup`.
- Sunday 09:00, the bank's rewrite of the archive.

Decisions needed.

- Rewrite plan. Owner: Lucía Brandt and Rafael Quintero. By tonight.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 2 days 20 hours 30 minutes from now.

Not yet known. What data the snapshot holds. Whether the loan platform's data is intact. Who the actor is. Whether anything leaves the bank at the deadline.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

Stage 3 Protect and recover: rewrite the archive, fill the vault

Every 12 hours, Sunday, July 5, to Monday, July 6. The bank rewrites the archive under its own keys while the vault fills and its protections are set.

SR-08: Sunday, July 5, 09:30 EDT (13:30 UTC)

As of: Sunday, July 5, 09:30 EDT (13:30 UTC). **Stage:** Stage 3 Protect and recover: rewrite the archive, fill the vault. **Report:** 8 of 16.

Headline. The month-end snapshots are back and the bank's own rewrite of the archive has started, in sequential slices.

Confirmed.

- The 9 month-end database snapshots were copied back from `wf-backup` into the lending account between 05:10 and 07:50, one every 20 minutes. They are the bank's own and sit under the bank's key.
- The role `s3-batch-restore` was created at 08:50. The bank's rewrite began with its first slice job at 08:58 and copying at 09:00. It is 31 sequential slice jobs, 30 of 2 million versions and the last of 1.3 million, each with a bucket key and a version-specific manifest. The rewrite is 1% done by its counters (about 0.6 million objects).
- The bank counted the applicant records in the source database for the shared snapshot: **412,317**, with names, Social Security numbers, dates of birth, and income. The split by state of residence will follow.
- The attacker's last call remains the denied `ListUsers` at 03:00 Saturday.

Working hypotheses (not confirmed).

- The bank's rewrite averages about 330 objects a second, far below the attacker's rate of about 4,500. The reason is the design: the slices run one after another, and each is checked before the next starts. Our working estimate, from the first half hour, is that it finishes around midday on Tuesday, under six hours before the keys expire.
- If the snapshot left, it holds every record the database held at 21:22 Friday.

Actions since the last report.

- 05:10 to 07:50, the nine snapshots restored (bank, Imani Castell).
- 08:50 and 08:58, the rewrite role and first slice job created. 09:00, the rewrite started.

Proposed, awaiting approval.

- **Before any copy into the vault:** give the vault copy role read on the bank's source keys, by key policy, and share each source snapshot with the vault account. Then, from 12:00, copy the live database snapshot first and each restored month-end snapshot after it into the vault under the vault keys, one at a time.
- From Monday 02:00, copy the 46 volume snapshots into the vault, and lock the copies in compliance mode.
- Set Vault Lock on the AWS Backup recovery point of the live database, once the copies are done.

Decisions needed.

- Approve the compliance-mode locks, which cannot be undone after their cooling-off periods. Owner: Mireille Danvers. By Monday 05:30 EDT for the volume snapshots, and by Monday 19:00 EDT for Vault Lock.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 2 days 8 hours 30 minutes from now.

Not yet known. Whether the rewrite will finish in time. Whether the outside account tries again. Whether the shared snapshot is in use.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

SR-09: Sunday, July 5, 21:30 EDT (July 6, 01:30 UTC)

As of: Sunday, July 5, 21:30 EDT (July 6, 01:30 UTC). **Stage:** Stage 3 Protect and recover: rewrite the archive, fill the vault. **Report:** 9 of 16.

Headline. The vault is being filled and the rewrite is on pace. The bank's trail shows nothing from the attacker since Saturday, and it could not show a denied try on the lending key.

Confirmed.

- The last call from the attacker's account that the bank's trail holds is the retirement of the grant on Saturday at 00:51 EDT. The resource control policy has been on since 03:20 that morning, and no outside use of the key has been allowed since. In all, 7 KMS calls from the outside account on that key reached the bank's trail, all in the copy-out burst between 00:06 EDT and 00:51 EDT on Saturday.

- The bank's review of the loan platform's application and load-balancer logs, collected this morning (`EVD-018`), shows no attacker traffic. We state it as what the bank found in the logs it has, not as proof that none occurred.
- 09:30 and 10:00, before the copies, the bank gave the vault copy role read on the source keys through three key policies, and shared the ten source database snapshots with the vault account.
- 4 of the 10 database snapshot copies into the vault are done (first at 12:00, then every 3 hours or so).
- The rewrite is 24% done by its counters (about 14.8 million of 61.3 million objects).

Working hypotheses (not confirmed).

- The attacker's account may have tried the lending key again. A request that the key policy or the resource control policy denies is logged only in the caller's account, which the bank does not hold, so the bank's trail cannot show a try either way. We do not state that one happened.
- Assumption: the resource control policy stops outside use of the key. Its evidence is its text and attachment (Saturday 03:19 and 03:20) and the absence of any allowed outside use since, not a logged deny.

Actions since the last report.

- 09:30 and 10:00, key policies updated and the ten database snapshots shared with the vault account (bank, Imani Castell).
- 12:00, 15:07, 18:14, and 21:21, snapshots copied into the vault (bank, Imani Castell).
- Rewrite running since 09:00, one slice job after another.

Proposed, awaiting approval.

- Sunday 22:00, share the 46 volume snapshots with the vault account. Monday 02:00, copy them into the vault.
- Delete nothing of the attacker's before preservation is complete. The plan is to remove the attacker's user, key, and roles on Wednesday morning, after the evidence is hashed and locked.
- Keep the three attacker keys, not deleted, for counsel.

Decisions needed.

- Approve that eradication sequence in principle. Owner: Mireille Danvers. By Tuesday 21:30 EDT.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 1 day 20 hours 30 minutes from now.

Not yet known. Whether the rewrite stays on pace. Whether the attacker has any other path. Anything the attacker plans at the deadline. The ransom contact has not been used.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

SR-10: Monday, July 6, 09:30 EDT (13:30 UTC)

As of: Monday, July 6, 09:30 EDT (13:30 UTC). **Stage:** Stage 3 Protect and recover: rewrite the archive, fill the vault. **Report:** 10 of 16.

Headline. The rewrite is about halfway and the vault copies are most of the way done. The volume snapshot copies are locked. No attacker call since Sunday afternoon.

Confirmed.

- The rewrite is 47% done by its counters (about 29.1 million objects).
- 7 of the 10 database snapshot copies are in the vault.
- The 46 volume snapshots were shared with the vault account at 22:00 Sunday. Their copies began at 02:00 and ended at about 05:22.
- **At 05:45 all 46 volume snapshot copies were locked in compliance mode** for 14 days, with a cooling-off period of 72 hours that ends Thursday, July 9, 05:45 EDT. After that the lock cannot be removed by anyone, including the bank and us.
- **The 10 database snapshot copies are ordinary snapshots and are not under any lock.** The lock covers the volume snapshot copies only. What protects the database copies is the vault OU policy, which denies their deletion, sharing changes, and key changes to everyone, and keys that only the bank holds.
- At 06:10 the AWS Backup vault `wf-recovery` was created, and at 06:40 a database `wf-los-vault` was restored in the vault account from the 21:22 Friday snapshot copy.
- We have seen no attacker call since Saturday at 03:00.

Working hypotheses (not confirmed).

- The rewrite will finish before the keys expire if the rate holds. A drop in the rate would be the early sign it would not.
- The attacker will move on once the deadline passes with no contact.

Actions since the last report.

- Sunday 22:00, the volume snapshots shared with the vault account. Monday 02:00 to about 05:22, copied into the vault.
- Monday 05:45, the 46 copies locked in compliance mode (Mireille Danvers approved, bank executed).
- Monday 06:10 and 06:40, the backup vault created and `wf-los-vault` restored.
- Monday 00:28, 03:35, and 06:42, three more database snapshots copied into the vault.
- Rewrite running.

Proposed, awaiting approval.

- Start an AWS Backup job on `wf-los-vault` this afternoon, then set Vault Lock on the backup vault in compliance mode, minimum retention 14 days, after the last copy is checked.

Decisions needed.

- Approve the Vault Lock at 19:00 EDT today. Owner: Mireille Danvers. By 19:00 EDT.
- Whether loan origination returns Wednesday afternoon, subject to integrity checks. Owner: Lucía Brandt, with Rafael Quintero. By Tuesday 21:30 EDT.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 1 day 8 hours 30 minutes from now.
- The volume snapshot locks leave their cooling-off period Thursday, July 9, 05:45 EDT.
- Loan origination offline 2 days 7 hours 40 minutes so far.

Not yet known. Whether the keys will expire as set. Whether the rewrite will meet the margin. Whether anything not in the trail has happened.

SR-11: Monday, July 6, 21:30 EDT (July 7, 01:30 UTC)

As of: Monday, July 6, 21:30 EDT (July 7, 01:30 UTC). **Stage:** Stage 3 Protect and recover: rewrite the archive, fill the vault. **Report:** 11 of 16.

Headline. The vault copies are complete, the live-database recovery point is locked, and the database copies rest on policy. Tuesday is the attacker's deadline.

Confirmed.

- The last database snapshot copy, of the June month-end snapshot, was logged at 16:03. The live snapshot was copied first, at 12:00 on Sunday. All 10 copies are logged in the vault.

- At 14:20 an AWS Backup job took one recovery point of `wf-los-vault`. At 19:30 Vault Lock was set on the backup vault in compliance mode with a 14-day minimum retention. It has a three-day cooling-off period, which ends Thursday, July 9, 19:30 EDT. After that the lock cannot be removed by anyone, including the bank and us.
- **Vault Lock protects that one recovery point of the live database. "Copied and locked" is true of the 46 volume snapshot copies only.** All 10 database snapshot copies remain ordinary snapshots under the vault OU policy and the bank's keys.
- The rewrite is 71% done by its counters (about 43.3 million objects).

Working hypotheses (not confirmed).

- The vault holds a complete, clean copy of the loan database as it stood on Friday night and of the month-end history. Verification so far is by the copy records and snapshot metadata, and by the restore of `wf-los-vault`, which we have not yet compared with the source.
- **The weakest link in the vault is a person.** Someone with Organizations rights in the management account could change the vault OU policy and then act on the database copies. The policy and the bank's keys stop everyone else.
- The rewrite is on pace to end around midday tomorrow.

Actions since the last report.

- 09:49, 12:56, and 16:03, the April, May, and June month-end copies.
- 14:20, the backup job on `wf-los-vault`.
- 19:30, Vault Lock configured (Mireille Danvers approved, Imani Castell executed).

Proposed, awaiting approval.

- Tomorrow 14:00, check that no current object in the archive is under any attacker key. The method: read the completion reports of the 31 slice jobs, and query the bucket's S3 Metadata live inventory table with Athena. S3 Inventory is a scheduled report and cannot be run on demand, so it is not the check.
- Do nothing at 18:00 except watch and record. We will not touch the expired keys.

Decisions needed.

- Confirm that no action is taken at the deadline except watching. Owner: Mireille Danvers. By Tuesday 09:00 EDT.
- Approve the Wednesday 10:00 eradication in sequence. Owner: Mireille Danvers. By Tuesday 21:30 EDT.

- Decide who may change the vault OU policy in the management account. Today anyone with Organizations rights there can. Owner: Mireille Danvers, with Imani Castell. By Tuesday 21:30 EDT.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 20 hours 30 minutes from now.
- The Vault Lock cooling-off ends Thursday, July 9, 19:30 EDT.

Not yet known. Whether the restored vault database matches its source. Whether the attacker acts at the deadline. Whether anything the bank needs is under the keys, which the 14:00 check will settle.

Stage 4 Eradicate: the deadline passes, the attacker's identities go

Every 12 hours, Tuesday, July 7, to Wednesday, July 8. The attacker's keys expire, the attacker's identities are removed after preservation, and loan origination returns.

SR-12: Tuesday, July 7, 09:30 EDT (13:30 UTC)

As of: Tuesday, July 7, 09:30 EDT (13:30 UTC). **Stage:** Stage 4 Eradicate: the deadline passes, the attacker's identities go. **Report:** 12 of 16.

Headline. The rewrite is nearly done with hours to spare before the keys expire.

Confirmed.

- The rewrite is 94% done by its counters (about 57.5 million objects). We expect it to finish around 12:40 EDT, which is 5 hours 20 minutes before the keys expire.
- Nothing from the attacker since Saturday 03:00.

Working hypotheses (not confirmed).

- The rewrite finishes before the deadline. If it does, no object the bank needs is current under an attacker key at 18:00.
- Any object still current under an attacker key at 18:00 would be unreadable after the material expires, though its bank-key version would remain.

Actions since the last report.

- The rewrite ran. The vault copies finished. Nothing else.

Proposed, awaiting approval.

- 14:00, read the completion reports of the 31 slice jobs and query the live inventory table for the current versions under any attacker key ARN and under the bank's key.
- If the check is not clean by 15:00, escalate and rewrite the remainder by hand.

Decisions needed.

- Go or no-go on the Wednesday eradication. Owner: Mireille Danvers. By 21:30 EDT.

Deadlines running.

- The attacker's deadline: Tuesday, July 7, 18:00 EDT, 8 hours 30 minutes from now.
- Vault Lock cooling-off ends Thursday, July 9, 19:30 EDT.

Not yet known. Whether the job finishes at its estimated time. Whether the check is clean. Whether the attacker acts at 18:00.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

SR-13: Tuesday, July 7, 21:30 EDT (July 8, 01:30 UTC)

As of: Tuesday, July 7, 21:30 EDT (July 8, 01:30 UTC). **Stage:** Stage 4 Eradicate: the deadline passes, the attacker's identities go. **Report:** 13 of 16.

Headline. The deadline has passed. The bank reports that its 14:00 check found no current object under the attacker's keys, and nothing was paid.

Confirmed.

- The rewrite finished at 12:40 EDT, having copied 61.3 million noncurrent bank-key versions back as current, in 31 slice jobs.

- At 14:00 the bank read the 31 completion reports of the slice jobs, which show 61,300,000 tasks succeeded and 0 failed. The bank first checked that the bucket's S3 Metadata live inventory table was current: its status was ACTIVE, and a canary object written at 13:20 showed up in a query at 13:50, so the table covered writes through 13:20, which is after the last slice finished at 12:40 (nobody assumed it had caught up). Then two Athena count queries over the table (`StartQueryExecution` at 13:52 and 13:55; the three queries are `EV-01034` to `EV-01036`) reported **0 current versions under any attacker key ARN** and 286,000,000 current versions under the bank's key. The 61,300,000 noncurrent versions under the attacker keys remain, and the bank does not need them. This count is bank-reported; the query results were not independently preserved, because the register holds the two query calls (which show submission, not a result) and not the result files. S3 Inventory is a scheduled report and cannot be run on demand, so it was not the method; a scheduled report would later confirm inventory and encryption-type coverage, not which KMS key encrypted each version.
- At 18:00 the imported key material expired on all three keys. KMS logged `DeleteExpiredKeyMaterial` for each (`EV-01037`, `EV-01038`, `EV-01039`). On that count, no current object is under them and nothing the bank needs is. The keys have been in the PendingImport state since 18:00.
- No payment was made, and the ransom contact was not used. There has been no contact from the attacker since the note.
- The attacker made no call at the deadline.

Working hypotheses (not confirmed).

- The attacker may turn to a second threat, publishing the data, if it was copied out. We have no evidence of that yet, and the bank should be ready for it.
- The attacker may leave. Their account has been quiet since Sunday.

Actions since the last report.

- 13:18 to 14:00, the canary check of the live inventory table, its two count queries, and the reading of the completion reports (bank, Imani Castell).
- The key material expired as set.

Proposed, awaiting approval.

- Wednesday 10:00, eradication in sequence: preserve, then remove the user, key, and roles, narrow the deploy role's trust, and replace the service user with an OIDC role. Keep the three attacker keys for counsel and delete nothing. At 10:03 the bank will call `DisableKey` on each attacker key and read the key with `DescribeKey` after, so the trail shows what was tried and the state the keys are left in. A key in PendingImport may reject the call.

Decisions needed.

- Approve the eradication. Owner: Mireille Danvers. By 09:30 EDT Wednesday.
- A holding statement in case the attacker publishes. Owner: Gregory Ashworth, with Harold Penwick.

Deadlines running.

- The attacker's deadline is over.
- Vault Lock cooling-off ends Thursday, July 9, 19:30 EDT.
- Loan origination offline 3 days 19 hours 40 minutes.

Not yet known. Whether the attacker will publish. Whether other footholds exist. How the key got out.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

SR-14: Wednesday, July 8, 09:30 EDT (13:30 UTC)

As of: Wednesday, July 8, 09:30 EDT (13:30 UTC). **Stage:** Stage 4 Eradicate: the deadline passes, the attacker's identities go. **Report:** 14 of 16.

Headline. Eradication is ready to start in half an hour, after preservation.

Confirmed.

- The evidence for each identity and key we will remove is exported, hashed, and locked in `wf-ir-evidence`.
- Nothing from the attacker since Saturday 03:00.
- Loan origination has been offline 4 days 7 hours 40 minutes.

Working hypotheses (not confirmed).

- The eradication takes about 15 minutes of the bank's work, then a check.
- Loan origination can return at 16:00 if the integrity checks pass.

Actions since the last report. None. The bank prepared the sequence.

Proposed, awaiting approval.

- 10:00, remove `aws-support-sync` (detach policy, delete key, delete user), `OrgAccessBackup`, and `s3-batch-replication`.

- 10:03, call `DisableKey` on each of the three attacker keys and read each key with `DescribeKey` after. The keys are in PendingImport, where KMS may reject the call. Keep them as they are, for counsel. Do not delete them.
- 10:05, narrow `wf-deploy-pipeline`'s trust in ten accounts to the Jenkins role, with a source identity condition.
- 10:10, delete `svc-artifact-sync` and its key, and create the OIDC provider that replaces it.

Decisions needed.

- Approve the eradication. Owner: Mireille Danvers. By 10:00 EDT.
- Go or no-go for loan origination at 16:00. Owner: Lucía Brandt, with Rafael Quintero. By 15:00 EDT.

Deadlines running.

- Loan origination offline, 4 days 7 hours 40 minutes and counting.
- Vault Lock cooling-off ends Thursday, July 9, 19:30 EDT.

Not yet known. Whether the integrity checks will pass. Whether removing the identities breaks a build.

SR-15: Wednesday, July 8, 21:30 EDT (July 9, 01:30 UTC)

As of: Wednesday, July 8, 21:30 EDT (July 9, 01:30 UTC). **Stage:** Stage 4 Eradicate: the deadline passes, the attacker's identities go. **Report:** 15 of 16.

Headline. The attacker's identities are gone, the deploy role is narrowed, and loan origination is back online. The attacker's keys stay in PendingImport; the calls to disable them were rejected.

Confirmed.

- The eradication ran from 10:00 to 10:11, after preservation. The attacker's user, second key, and two roles are deleted. The three attacker keys are kept for counsel and not deleted. Their imported material expired Tuesday at 18:00, so they have been in the PendingImport state since.
- **No key change succeeded on Wednesday.** The bank's `DisableKey` calls on the three attacker keys, at 10:03:30, 10:03:55, and 10:04:20, were each rejected with `KMSInvalidStateException` (`EV-01052`, `EV-01054`, `EV-01056`), and the `DescribeKey` after each returned the key as `PendingImport` and not enabled. KMS rejects `DisableKey` for a key in that state. The rejected calls are in the trail. The keys stay in PendingImport and are kept as they are, for counsel. The outside account's statement was dropped from each key policy on Saturday at 02:09 (`PutKeyPolicy`), not on Wednesday.

- `wf-deploy-pipeline`'s trust was narrowed in all ten workload accounts between 10:05 and 10:08.
- `svc-artifact-sync` and `AKIAWRFNEXAMPLE00001` were deleted at 10:10, and an OIDC provider created at 10:11 to replace them.
- **Loan origination came back online at 16:00**, after integrity checks, having been offline 110 hours 10 minutes. 1,912 applications queued meanwhile, and the bank expects to process them by Friday.
- At 16:30 a bucket with Object Lock was created in the vault, and at 17:05 a replication rule from the imaging archive into it was put in place. A rule copies only objects written after it exists, so for the existing objects the bank built a manifest at 18:12 with an Athena `UNLOAD` over the live inventory table (the current versions under the bank's key), and at 18:25 started an S3 Batch Replication job (`s3ReplicateObject`, `EV-01101`) over it, with its completion report enabled. The job's description names 286,000,000 current versions.

Working hypotheses (not confirmed).

- The archive's copy in the vault is not complete yet. The job started at 18:25, and with that many versions we expect it to run for days, not hours. The manifest holds current versions only; versions that are not current are not in it.
- Removing the identities has closed every foothold we know. Only the sweep can say whether we know them all.

Actions since the last report.

- 10:00 to 10:11, eradication and trust narrowing (Mireille Danvers approved, Imani Castell executed).
- 16:00, loan origination back online (bank).
- 16:30, 17:05, 18:12, and 18:25, the vault archive bucket, the replication rule, the manifest query, and the replication job (Imani Castell).

Proposed, awaiting approval.

- Tomorrow, declare containment in writing, with the vault copy of the archive named as an open item.
- The Investigation and the Recovery from Monday, July 13.

Decisions needed.

- Declare containment. Owner: Mireille Danvers. Thursday 09:00 EDT.
- Whether to engage the Investigation and the Recovery. Owner: Mireille Danvers, with Diane Whitcombe. By Friday, July 10.

Deadlines running.

- Vault Lock cooling-off ends Thursday, July 9, 19:30 EDT.
- The 1,912 queued applications, which the bank expects to process by Friday.

Not yet known. When the replication job finishes, whether any of its tasks fail, and whether the vault copy of the archive can then be checked. Whether any foothold remains. The root causes in full. Whether the shared snapshot's data has been used.

Stage 5 Containment declared

Thursday, July 9. The last report of the Response.

SR-16: Thursday, July 9, 09:30 EDT (13:30 UTC)

As of: Thursday, July 9, 09:30 EDT (13:30 UTC). **Stage:** Stage 5 Containment declared. **Report:** 16 of 16.

Headline. Containment is declared in writing. This is the last report of the Response.

Confirmed.

- At 09:00 Mireille Danvers declared containment in writing. The Response ends with this report. Effort for the Response was 56 hours in total.
- The attacker's last call in the bank's trail was a denied `ListUsers` on Saturday at 03:00. No call since. A try by the attacker's own account on a key would be logged only in that account, so this trail would not show it.
- The state of the estate: the attacker's known credentials are gone, the imported material of the three attacker keys has expired and the keys are kept for counsel, no current object is under an attacker key on the bank's 14:00 count (bank-reported), the guardrail policies stand, and loan origination is online.
- The exfiltration path was closed on Saturday, July 4: the share at 02:08:20 EDT, the key statements at 02:09, and the grant at 02:10:30 EDT.
- The vault holds the 46 locked volume snapshot copies, the 10 database snapshot copies under policy, and one locked recovery point of the live database.
- The vault copy of the imaging archive is not complete. The S3 Batch Replication job over the current versions under the bank's key started Wednesday at 18:25 and is still running; no completion report is in yet. Its finish, any failed tasks, and a read-back of the vault bucket stay open items.

- Items stay open: deletion protection on `wf-los-prod` is off, the deleted legacy trail is not recreated, and the vault OU policy can still be changed by anyone with Organizations rights in the management account. The containment report lists them, and the Recovery takes them up in week three.

Working hypotheses (not confirmed).

- The attacker has left. That is a belief, and the sweep in the fourth week of the Recovery is what tests it.
- The data copied out, if it was, will be used or offered for sale. No sign yet.

Actions since the last report.

- 09:00, containment declared (bank).

Proposed, awaiting approval.

- The Investigation and the Recovery, four weeks from Monday, July 13.

Decisions needed.

- Sign the Investigation and the Recovery. Owner: Mireille Danvers, with Diane Whitcombe. By Friday, July 10, 2026.

Deadlines running.

- Vault Lock cooling-off ends Thursday, July 9, 19:30 EDT, tonight.
- The volume snapshot copies stay locked until Monday, July 20, 2026.

Not yet known. When the replication job into the vault finishes, and what it reports as failed. Whether data left, beyond "probable." Whether the attacker is out, beyond our belief. How the key left the bank. All the root causes. Those are the work of the Investigation.

Counsel items. Counsel items for this report are in the counsel notes in the clock worksheet (Report 4).

Notice

Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

© 2026 Vantalect, LLC. Sample deliverable; Wrenfield Bancorp, Inc. is fictional.

AWS, Amazon Web Services, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. MITRE ATT&CK is a registered trademark of The MITRE Corporation. PostgreSQL is a registered trademark of the PostgreSQL Community Association of Canada. Other product names are trademarks of their owners. Vantalect is not affiliated with or endorsed by any of them. Wrenfield Bancorp, Inc. is fictional.