Vantalect



AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

Estate Map and Evidence Preservation

DISTRIBUTION: COUNSEL ONLY

Week 1 of 4: Preserve and map · prepared for Wrenfield Bancorp, Inc.

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

July 17, 2026 · AWS Breach Forensics & Recovery: The Investigation and the Recovery (four weeks)

SAMPLE DELIVERABLE

Privileged and confidential. Prepared at the direction of counsel. Sample. Wrenfield is fictional.

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

Scope and what this report is 2

Limits of the evidence 3

The organization 5

The accounts 7

Policies and guardrails 10

Delegated administrators and organization services 12

Identities and trust paths 12

Principals 13

Cross-account trust paths 15

Federation 16

Keys 17

Data stores in scope 20

Network exposure 23

Log sources 25

The preservation record 27

What week 1 leaves for week 2 32

Notice 32

Scope and what this report is

This report maps the bank's AWS estate as it stood at the end of week 1 and lists what was preserved, so that every claim in the weeks that follow has a source. It covers the Investigation's first week, July 13 to July 17, and is dated Friday, July 17, 2026. It states only what week 1 knew. It draws no conclusion about how the attacker got in, why the attack worked, or what it reached; that is the work of week 2, and its readout is on Friday, July 24.

Privileged and confidential. Prepared at the direction of counsel. The label does not protect a document by itself: privilege depends on how and why the work was commissioned, and counsel decides whether it applies. Vantalect makes no determination about privilege. The distribution line, **Counsel only**, means this report goes to Diane Whitcombe of Tessaly & Brook LLP and to the bank's Chief Information Security Officer, Mireille Danvers. Counsel decides who sees it after that.

How to read it. The report describes the estate "as found" on July 3, then what changed during the response (July 4 to 9) and in week 1, and it marks which is which. The limits of the evidence come first, in the next section, so that nothing after them is read as stronger than it is. Where a statement rests on a sealed evidence item, the item's ID is given (`EVD-001` and so on); the full register is in the Chain-of-Custody Log. Vantalect makes no determination that anything in this report is a breach, a notification trigger, or privileged; those are the bank's and counsel's decisions.

The estate has 22 accounts in one organization: the 20 that existed on July 3 and the two the response added, `wf-ir-forensics` and `wf-recovery-vault`. Two Regions are in use: US East (N. Virginia) as primary and US East (Ohio) for disaster recovery.

Limits of the evidence

Eight limits bound everything this report and the later ones can say. Each is a fact about what was logged, collected, or reachable, not a doubt about any particular item.

The limits of the evidence, part 1 of 2.

Limit	What it means	Effect on later claims
Object reads from the imaging archive were not logged	S3 data events on the imaging and data-lake buckets record writes only. Whether any object was read, by anyone, is unknown, and no evidence item can show it.	Any later statement about reads will say "unknown" or give the indirect evidence and its limit. It will not say "none."
The lending documents bucket has no data events	Its ransom note is evidenced by the object's metadata and the bucket listing (`EVD-004`), not by a trail record.	Writes to this bucket cannot be dated or attributed from the trail.
No read-only management events reach an alert path	The organization trail records them, so they are evidence, but nothing watched them as they happened.	The trail can show the discovery calls after the fact. It cannot show whether anyone saw them then.
Nothing outside AWS is in the register	Endpoints, the core banking service bureau, and any device a contractor used are outside what Vantalect can read.	Claims about how a credential left the bank, if made at all, will rest on other sources and say so.

The limits of the evidence, part 2 of 2.

Limit	What it means	Effect on later claims
The attacker's account is closed to us	Account `777788889999` is not ours or the bank's. What happened inside it is visible only through the calls it made into the bank's accounts.	A call the attacker made inside its own account leaves no record we can read.
The legacy account trail was deleted	`wf-lending-legacy-trail` was deleted at 22:14 on July 3 (`EV-00501`). The organization trail recorded the deletion and still records everything else.	The trail's configuration was deleted and its delivery stopped. Log files it had already delivered remain unless separately deleted, and no such deletion is shown. The organization trail covers every account.
No host image was taken	The registers hold the Jenkins controller's and the loan platform's logs, not disk or memory images of any instance.	A question that only a host image answers will be answered from logs, with its limits stated.
Sealed copies are of the logs as delivered	The trail's digest chain validates the sealed files. It does not show that every event reached the trail.	Absence of an event is weaker evidence than its presence.

Two of these limits are the plainest and the most likely to be misread. **Object reads from the imaging archive are unknown, because reads were not logged.** An absence of evidence of reads is not evidence that there were none. And the **sealed trail is complete as delivered**: it shows every event CloudTrail recorded and delivered, and its digest chain validates, but it cannot show an event that was never recorded.

The organization

The organization `o-wrnfld4x7q` has 22 accounts, and the management account holds no workloads. The OUs and the accounts in each are below, then the policies that apply to them and the services administered from other accounts.

The root and the OUs, with the number of accounts in each.

OU	Accounts	What it holds
Root (`r-wrnf`)	1	The management account only. It holds no workloads.
Security	2	Log archive and audit. The organization trail's bucket and the delegated security services.
Infrastructure	5	Network, shared services, identity, tools, and the central backup vault.
Workloads (Prod and NonProd) (`ou-wrnf-wl000001`)	10	The parent of the two workload OUs: five production and five non-production accounts.
Sandbox	2	Two accounts for the platform and application teams.
Incident (`ou-wrnf-ir000001`)	1	Created at 03:11 on July 4 (`EV-00647`) for the evidence account.
Recovery (`ou-wrnf-rc000001`)	1	Created at 04:29 on July 4 (`EV-00658`) for the recovery vault.

The accounts

The 22 accounts, with owner and purpose. The two marked "added July 4" are the response's: the evidence account and the recovery vault.

The accounts, part 1 of 3.

Account	ID	OU	Owner	Purpose
`wf-management`	584729103301	Root	Imani Castell	Organization management, consolidated billing, and policies; no workloads
`wf-log-archive`	584729103314	Security	Mireille Danvers	The organization trail (management events, plus write-only S3 data events on the imaging and data-lake buckets)
`wf-audit`	584729103322	Security	Mireille Danvers	Delegated GuardDuty, Security Hub, and Config; alerts go to the managed security service provider
`wf-network`	584729103337	Infrastructure	Imani Castell	Transit gateway, egress inspection, and the connections to the core banking service bureau
`wf-shared-services`	584729103345	Infrastructure	Imani Castell	Directory, DNS, and artifact mirrors
`wf-identity`	584729103351	Infrastructure	Imani Castell	IAM Identity Center delegated administration
`wf-tools`	584729103358	Infrastructure	Imani Castell	Jenkins and the artifact sync job; the compromised IAM user lives here
`wf-backup`	584729103366	Infrastructure	Imani Castell	The central AWS Backup vault (Vault Lock in governance mode)

The accounts, part 2 of 3.

Account	ID	OU	Owner	Purpose
wf-prod-lending	584729104402	Workloads/Prod	Lucía Brandt	Loan origination: RDS for PostgreSQL wf-los-prod (2.1 TB) and the EC2 application tier
wf-prod-imaging	584729104415	Workloads/Prod	Rafael Quintero	The document imaging archive: loan files, check images, and signature cards (S3, 286 million objects, 412 TB)
wf-prod-data	584729104423	Workloads/Prod	Rafael Quintero	The data lake
wf-prod-digital	584729104438	Workloads/Prod	Rafael Quintero	Digital account opening and the online-banking middleware
wf-prod-treasury	584729104446	Workloads/Prod	Rafael Quintero	The treasury management portal
wf-nonprod-lending	584729105502	Workloads/NonProd	Lucía Brandt	Lending development and test
wf-nonprod-imaging	584729105515	Workloads/NonProd	Rafael Quintero	Imaging development and test
wf-nonprod-data	584729105523	Workloads/NonProd	Rafael Quintero	Data lake development and test

The accounts, part 3 of 3.

Account	ID	OU	Owner	Purpose
`wf-nonprod-digital`	584729105538	Workloads/NonProd	Rafael Quintero	Digital development and test
`wf-nonprod-treasury`	584729105546	Workloads/NonProd	Rafael Quintero	Treasury development and test
`wf-sandbox-1`	584729106601	Sandbox	Imani Castell	Platform sandbox
`wf-sandbox-2`	584729106615	Sandbox	Imani Castell	Application team sandbox
`wf-ir-forensics` (added July 4)	584729107701	Incident	Mireille Danvers	Evidence preservation under S3 Object Lock; created at 03:12 on July 4, owned by the incident role
`wf-recovery-vault` (added July 4)	584729107714	Recovery	Mireille Danvers	The recovery vault behind a deny-all SCP except two copy roles; keys held by the bank (created at 04:30 on July 4)

Policies and guardrails

On July 3 the organization's only service control policy was the AWS default. Every guardrail below was added on or after July 4. Before 01:22 on July 4, no SCP or RCP restricted key origin, imported key material, snapshot sharing, lifecycle changes, or S3 Batch jobs. That is the configuration as found; whether it mattered is a question for week 2.

The policies in force on July 17.

Policy	ID	Type	Attached to	Since	What it does
`FullAWSAccess`	AWS managed default	SCP	Root and every OU	2021	Allows everything. The deny policies below layer on it.
`wf-incident-containment`	p-wrnfcontain01	SCP	Workloads OU	01:22 July 4 (`EV-00537`); updated 02:58 (`EV-00642`)	Denies key import and deletion, key policy and grant changes, non-AWS key origins, snapshot deletion and sharing, DB instance changes, lifecycle, versioning, and trail changes, IAM user, key, and role creation, and S3 Batch job creation. The incident role and the break-glass role are exempt. A second statement denies the three attacker principals everything.
`wf-deny-outside-access`	p-wrnfrcp00001	RCP	Workloads OU	03:20 July 4 (`EV-00654`); policy type enabled at 03:15, outside trusts listed with Access Analyzer at 03:16	Denies `sts:AssumeRole` (and the related STS actions), `kms:*`, and `s3:*` to any principal outside the organization, except AWS services. The STS statement exempts one named user, `arn:aws:iam::111122223333:user/charles-sieg`. The KMS statement is what denied the attacker's account on July 5.
`wf-evidence-deny-all`	p-wrnfevid00001	SCP	Incident OU	03:52 July 4	Denies everything except the custodian's role, `wf-evidence-custodian`.

Policy	ID	Type	Attached to	Since	What it does
`wf-vault-deny-all`	p-wrnfvault0001	SCP	Recovery OU	04:34 July 4 (`EV-00663`)	Denies everything except two copy roles, `wf-vault-copy-in` and `wf-vault-copy-out`, each assumed with MFA and two-person approval. A second statement denies everyone, those roles included, snapshot deletion, snapshot sharing changes, snapshot unlocking, and key deletion, disabling, policy changes, and grant revocation. As created it also exempted the account's `OrganizationAccountAccessRole` (the bank's setup role, with `AdministratorAccess`, trusted by the management account), which made the vault's keys, snapshot locks, Backup vault, and Vault Lock from July 4 to July 6 and the archive key on July 8. The update at 16:45 on July 8 (`EV-01092`) removed it from the list, so it is denied by name. The trail shows no later change as of July 17. Anyone with Organizations rights in the management account can still change this SCP.

Delegated administrators and organization services

Delegated administrators and where each organization service is run.

Service	Administered from	Notes
GuardDuty, Security Hub, and AWS Config	`wf-audit`	Findings go to the managed security service provider. Config's aggregator is `wf-org-aggregator`.
IAM SAML provider	`wf-management`	Workforce sign-in through the bank's identity provider, `wrenfield-idp`, into the role `wf-saml-platform-admin`.
CloudTrail (organization trail `wf-org-trail`)	`wf-management`	Created in the management account; its bucket is in `wf-log-archive`.
CloudFormation StackSets	`wf-management`	Not delegated. `VantalectIncidentResponse` was deployed by a self-managed StackSet created here at 01:31 on July 4 (`EV-00567`).

Identities and trust paths

The identities that matter are two IAM users, one build-pipeline role in ten accounts, and the roles the response added. Each is listed below with its state as found and its state on July 17. The three principals the attacker created or used as a base are marked, and each was captured before it was changed or deleted (`EVD-021`).

Principals

The principals in scope, part 1 of 2.

Principal	Kind	Account	What it is	State on July 17
`svc-artifact-sync`	IAM user	wf-tools	The artifact sync job's user. One long-lived access key, `AKIAWRFNEXAMPLE00001`, created March 14, 2023 and never rotated (as found).	Key set Inactive at 01:24 on July 4 (`EV-00543`). User and key deleted on July 8 at 10:10. Replaced by an OIDC role.
`aws-support-sync`	IAM user	wf-prod-data	Created by the attacker at 22:31 on July 3 with `AdministratorAccess` and key `AKIAWRFNEXAMPLE00002`.	Key set Inactive at 03:01 on July 4. User and key deleted on July 8 at 10:00 and 10:01. Captured first (`EVD-021`).
`wf-deploy-pipeline`	IAM role	The ten workload accounts	The build pipeline's deploy role. `AdministratorAccess`. Trust as found: the `wf-tools` account, with no conditions.	Sessions revoked at 01:26 on July 4. On July 8 at 10:05 to 10:08 the trust was narrowed to the Jenkins role with a source identity condition.
`wf-jenkins-agent`	IAM role	wf-tools	The role the Jenkins agents run as.	In use.
`OrgAccessBackup`	IAM role	wf-prod-lending	Created by the attacker at 22:36 on July 3. Trusts account `777788889999`.	Deleted July 8 at 10:02. Captured first (`EVD-021`).

The principals in scope, part 2 of 2.

Principal	Kind	Account	What it is	State on July 17
`s3-batch-replication`	IAM role	wf-prod-imaging	Created by the attacker at 21:39 on July 3. Trusts S3 Batch Operations.	Deleted July 8 at 10:03. Captured first (`EVD-021`).
`wf-break-glass`	IAM role	All 20 accounts that existed before the response	The bank's emergency access role. Exempt from the containment SCP.	Used by the bank's responders and as the StackSet execution role, which the SCP exempts, July 4 to 8 (50 sessions in 20 accounts, from 01:23 on July 4 to 17:04 on July 8). It removed the outside share and revoked the attacker's grant at 02:08 to 02:10 on July 4. In use.
`VantalectIncidentResponse`	IAM role	The same 20 accounts	Read-focused incident role, deployed by a self-managed StackSet at 01:39 and 01:40 on July 4 (the management account's copy by a separate stack at 01:40). Trusts one named principal, `arn:aws:iam::111122223333:user/charles-sieg`, not the account root.	In use for the engagement. The two accounts added on July 4 have no Vantalect role: both were created after the StackSet ran, and the evidence account's only exempt role is the bank's custodian role.
`wf-saml-platform-admin`	IAM role trusted by a SAML provider	wf-management	The platform lead's workforce role, reached by SAML from the IAM SAML provider `wrenfield-idp`.	In use.

Cross-account trust paths

Five trust paths cross an account boundary. The first is the one the response narrowed. The role `wf-deploy-pipeline` exists in the ten workload accounts and carries `AdministratorAccess`; as found, its trust policy named the whole `wf-tools` account with no conditions. That is the configuration, stated as found. How it was or was not used is week 2's question, and this report does not answer it.

The cross-account trusts, as found and now.

Role	Trusts	As found	On July 17
wf-deploy-pipeline (ten accounts)	Account `584729103358` (`wf-tools`)	Whole account. No conditions.	The `wf-jenkins-agent` role, with a source identity condition (July 8).
OrgAccessBackup (`wf-prod-lending`)	Account `777788889999` (outside the organization)	Created by the attacker. Unconditioned.	Deleted (July 8).
s3-batch-replication (`wf-prod-imaging`)	The S3 Batch Operations service	Created by the attacker.	Deleted (July 8).
VantalectIncidentResponse (20 accounts)	One named principal in Vantalect's account `111122223333`: the user `charles-sieg`	Deployed July 4. Exempt from the containment SCP. The RCP's STS statement exempts that one user.	In use.
OrganizationAccountAccessRole (the two new accounts)	The management account	Created with each new account (03:12 and 04:30 on July 4).	Blocked in `wf-ir-forensics` by its deny-all policy. In `wf-recovery-vault` it has `AdministratorAccess` and was used for the vault's setup (keys, snapshot locks, Backup vault, Vault Lock) from July 4 to July 6 (`EV-00667` to `EV-00998`) and for the archive key on July 8. The vault SCP exempted it until 16:45 on July 8 (`EV-01092`), when the update denied it by name. It still trusts the management account, but the SCP now stops it.

Federation

- **SAML 2.0 workforce federation.** The bank's identity provider, `wrenfield-idp`, is an IAM SAML provider; Identity Center is not used. The platform lead's sign-ins appear as `AssumeRoleWithSAML` of `wf-saml-platform-admin` in `wf-management`. A SAML session carries no `aws:MultiFactorAuthPresent` value, so the trail cannot show whether the identity provider required MFA.
- **OpenID Connect for the build.** Provider `https://token.jenkins.wrenfield.example`, created July 8 at 10:11 (`EV-01077`) to replace the long-lived key.
- **Cross-account role chains.** The build pipeline reached the workload accounts by role from `wf-tools`. Every workload account has a `wf-deploy-pipeline` role.

Keys

KMS keys fall into four groups by origin, and only one group, three keys with imported key material, was made by the attacker. The attacker's three keys are in the bank's own accounts and carry the alias `alias/wf-backup-2026`. Their material was set to expire at 22:00 UTC on July 7, which is 18:00 EDT, and it did. The key policies and metadata are sealed (EVD-007, EVD-008, EVD-009), and the keys were kept as they are, for counsel. Their material expired as set, which put each key in the `PendingImport` state (AWS logged `DeleteExpiredKeyMaterial` for each at 18:00 on July 7), and the outside statement in each key policy had been dropped on July 4 at 02:09. On Wednesday, July 8, at 10:03 to 10:04, the bank's `DisableKey` call on each key was rejected with `KMSInvalidStateException` (EV-01052, EV-01054, EV-01056), because a key in `PendingImport` cannot be disabled. No change to these keys succeeded on July 8, and they remain in `PendingImport`.

KMS keys by origin, with their policies and state.

Origin	KeysWhere	Policy	State
EXTERNAL (imported material)	3 `wf-prod-lending`, `wf-prod-imaging`, `wf-prod-data`, all aliased `alias/wf-backup-2026`	As found: the default root statement plus a statement naming account `777788889999`. The outside statement was dropped from all three on July 4 at 02:09 (`EV-00633` to `EV-00635`).	Created by the attacker July 3 at 21:06 to 21:10. Material valid to 2026-07-07T22:00:00Z; it expired at 18:00 EDT on July 7 (`EV-01037` to `EV-01039`), which moved each key to PendingImport. On July 8 at 10:03 to 10:04 the bank's `DisableKey` call on each key was rejected with `KMSInvalidStateException` (`EV-01052, EV-01054, EV-01056`): a key in PendingImport cannot be disabled, and no change to the keys succeeded that day. Kept as they are, for counsel. Captured as `EVD-007` to `EVD-009`.
AWS_KMS, bank keys	Not `alias/wf-rds` (the countedloan database) and in week 1 `alias/wf-imaging-bank` (the imaging archive), among others	Default policy; read from `EVD-026`.	In use. The imaging objects the attacker re-encrypted were rewritten under `alias/wf-imaging-bank`.
AWS_KMS, vault keys	3 `wf-recovery-vault`, alias `alias/wf-vault`	Held by the bank. Used only by the two vault copy roles.	Created at 04:40 on July 4 (`EV-00667` to `EV-00669`).
AWS_KMS, evidence key	1 `wf-ir-forensics`, alias `alias/wf-ir-evidence`	Administered by the bank. Vantalect holds no role in the account.	Created at 03:46 on July 4.

Grants.

- Two grants were created on the prod-lending attacker key at 00:06 on July 4 by a principal in account `777788889999` (`EV-00522` to `EV-00524`): one naming the attacker's role `exfil-runner`, and one naming the database service with `exfil-runner` as retiring principal. The second was retired at 00:51 (`EV-00531`). The first was revoked at 02:10 (`EV-00636`) after the grants on all three keys were listed (02:04 to 02:05, `EV-00629` to `EV-00631`).
- Every key's grants were read into `EVD-026`. Week 2 reads them against the trail.

Data stores in scope

Seven data stores are in scope, and the three that matter most are the loan database, the imaging archive, and the data lake. The loan database `wf-los-prod` is 2.1 TB in `wf-prod-lending`. The imaging archive `wf-imaging-archive-prod` holds 286,000,000 objects and 412 TB in `wf-prod-imaging`, with versioning on and no Object Lock as found. The data lake is `wf-datalake-prod` in `wf-prod-data`.

The data stores in scope, part 1 of 2.

Data store	Account	Size	Holds	Protection
RDS for PostgreSQL `wf-los-prod`	`wf-prod-lending`	2.1 TB	Loan origination: the applicants' records, which include names, Social Security numbers, dates of birth, and income.	Key `alias/wf-rds`. Nine month-end manual snapshots in the account, with copies in `wf-backup`. Deletion protection was turned off at 00:47 on July 4 (`EV-00529`) and is still off on July 17. The containment SCP denies `rds:ModifyDBInstance` and `rds:DeleteDBInstance` in the workload accounts, and it is the compensating control until the bank turns protection back on. The attacker-key snapshot copy `wf-los-prod-bk-20260703` was shared with account `777788889999` at 23:51 on July 3 (`EV-00520`). The share was removed at 02:08 on July 4 (`EV-00632`), 137 minutes after it was made; the attributes were captured first (`EV-00625`, `EVD-015`).
S3 bucket `wf-imaging-archive-prod`	`wf-prod-imaging`	286,000,000 objects, 412 TB	Loan files, check images, and signature cards.	Versioning on. No Object Lock (as found). Key `alias/wf-imaging-bank`. A replication rule (July 8 at 17:05) copies new writes to `wf-imaging-archive-vault`, an Object Lock bucket in the recovery vault. A rule alone copies only objects written after it exists, so at 18:12 the bank built a manifest with an Athena UNLOAD of the current versions under its key and at 18:25 EDT started an S3 Batch Replication job over them. The job finished at 21:40 EDT on July 12, 4 days 3 hours 15 minutes later: 286,000,000 current versions in the manifest, 1,206 tasks failed (`SrcVersionNotFound`: the version was gone from the source), and the 122,600,000 noncurrent versions (61,300,000 of them under attacker keys) were not in the manifest, so this job did not copy them.
S3 bucket `wf-datalake-prod`	`wf-prod-data`	Not measured in week 1	The data lake.	Server-side encryption with a bank key. Write data events on.
S3 bucket `wf-lending-docs-prod`	`wf-prod-lending`	Not measured in week 1	Lending documents.	No data events.

The data stores in scope, part 2 of 2.

Data store	Account	Size	Holds	Protection
EBS snapshots (46)	`wf-prod-lending` and `wf-prod-data`	31 in `wf-prod-lending` and 15 in `wf-prod-data`	Volumes of the loan platform's application tier and the data lake.	Recycle Bin rule, 10 days, in the production accounts. All 46 were restored on July 4.
Central backup vault	`wf-backup`	Not measured in week 1	Copies of the nine month-end RDS snapshots.	Vault Lock in governance mode.
Recovery vault `wf-recovery`	`wf-recovery-vault`	Not measured in week 1	Ten database snapshot copies (the nine month-end snapshots and the live-database snapshot), the 46 EBS snapshot copies, and one AWS Backup recovery point of a restored copy of the live database (`wf-los-vault`).	Three different protections. The 46 EBS copies were under snapshot lock in compliance mode for 14 days (a 72-hour cool-off) from July 6, which ended July 20 with no extension evidenced. The ten database copies are plain snapshots and are not under any lock; the vault SCP (which also denies deletion and key changes to everyone) and keys the bank holds are what protect them. Vault Lock (14-day minimum retention, 3-day cool-off) covers only the one recovery point in the Backup vault `wf-recovery`. The weakest link is a person with Organizations rights in the management account, who could change the SCP, or with administrator access there, who could enter the vault through the setup role.

Of the imaging archive's 286,000,000 objects, 61,300,000 (21.4%) had a current version under an attacker key when the attacker's S3 Batch job was canceled at 01:28 on July 4. The bank rewrote them under its own key in 31 sequential slice jobs, finishing at 12:40 on July 7. The bank checked the result at 14:00 EDT on that day from the 31 jobs' completion reports (61,300,000 tasks succeeded, 0 failed) and from 4 Athena queries, begun at 13:50 EDT, on the bucket's S3 Metadata live inventory table, which showed 0 current business-data object versions under any attacker key (the preserved ransom-note versions are excluded) and 286,000,000 under the bank's key (EVD-020). The scheduled S3 Inventory report of July 7 is in the same item as corroboration only, because a scheduled report is not run on demand and does not show the bucket after the rewrite finished; the next scheduled report, on July 8, is a later confirmation that is not an item in the register. The attacker's job was set up with its completion report off, so the job's own counters at cancellation are the record (EVD-017).

Network exposure

The attacker needed no network path into any host to do what the trail shows: every call was an API call, with a valid credential, to an endpoint that is public by design. That is a statement about how the AWS management plane works, not a finding about the bank. The table lists what is exposed and what week 1 knew about it.

Network exposure by area.

Area	Exposure	What week 1 knew
The management plane	AWS API endpoints are reachable from the internet by design. A valid credential is the only gate.	Every call the attacker made into the bank's accounts came from an internet address. Since 03:20 on July 4 an RCP denies STS role assumption, KMS, and S3 calls from principals outside the organization (AWS services excepted).
Loan origination	Web and application tier behind an Application Load Balancer in `wf-prod-lending`. Taken offline at 01:50 on July 4 and back at 16:00 on July 8.	Application and load-balancer logs are sealed (`EVD-018`). They are read in week 2.
Digital account opening, online banking, and treasury	Customer and staff endpoints in `wf-prod-digital` and `wf-prod-treasury`.	Listener and security group settings are in `EVD-027`. No log from these accounts has been read for network questions.
Core banking	Not in AWS. Reached through the service bureau connections in `wf-network` (transit gateway and egress inspection).	Out of scope for the Investigation.
Object storage	S3 public-access settings for the buckets in scope are in `EVD-027`.	Week 1 found no sign that any bucket in scope was open to the internet.
Flow logs and DNS logs	Their configuration is in `EVD-027`.	No flow log or DNS log was collected in week 1.

Addresses we hold for matching. All come from ranges reserved for documentation. The three attacker addresses are the ones in the trail.

Addresses used to match log lines.

Address	Belongs to
`198.51.100.23`	Attacker, first discovery calls
`198.51.100.41`	Attacker, second discovery period
`203.0.113.47`	Attacker, the production sessions and the second key
`198.51.100.200`	Wrenfield, outbound NAT
`203.0.113.210`	Wrenfield, VPN
`203.0.113.215`	Vantalect, incident work

Log sources

The estate has twelve log sources, and each has a gap that a later claim must respect. The organization trail records management events for every account and write-only S3 data events on the imaging and data-lake buckets. Read-only management events are recorded in the trail but not routed to the SOC, and there are no read data events. GuardDuty and Config add findings and resource state. The table gives, for each source, what it covers, how long it is kept, how it is delivered, how its integrity is shown, and its gap.

The log sources, part 1 of 3.

Source	Coverage	Retention	Delivery	Integrity	Gap
Organization trail `wf-org-trail`, management events	All accounts, both Regions. The two accounts added on July 4 from creation.	Kept in `wf-org-trail-logs`; 13-month expiry rule.	S3 in `wf-log-archive`.	Log-file validation on. Digest files. Encrypted. Separate account.	Read-only events are recorded but not routed to the SOC.
Organization trail, S3 data events	`wf-imaging-archive-prod` and `wf-datalake-prod`, writes only.	As the trail.	As the trail.	As the trail.	No read data events. No data events on the lending documents bucket.
Legacy trail `wf-lending-legacy-trail`	Account `wf-prod-lending` only.	Not applicable.	Not applicable.	Not applicable.	Deleted by the attacker at 22:14 on July 3. Its own files are not in evidence.
GuardDuty	All accounts, from the delegated administrator `wf-audit`.	90 days in the service; exported to `EVD-005`.	To Security Hub, then to the managed security service provider.	Generated by the service. The export is hashed.	The incident record holds one finding for the anomalous IAM activity, at 22:44 on July 3. Whether earlier findings exist is read from `EVD-005` and the provider's queue in week 2.

The log sources, part 2 of 3.

Source	Coverage	Retention	Delivery	Integrity	Gap
Security Hub	All accounts, aggregated in `wf-audit`.	Up to 90 days; exported to `EVD-005`.	To the provider's queue, which paged the on-call engineer at 23:18.	Generated by the service. The export is hashed.	Only findings, not events: it cannot show what GuardDuty did not raise.
AWS Config	Recorders per account; aggregator `wf-org-aggregator` in `wf-audit`.	Seven years (service default).	S3 and the aggregator.	Generated by the service. The snapshot is hashed (`EVD-014`).	Resource state, not API calls. Resource types recorded are listed in `EVD-027`.
KMS operations	Every call on a key, through the trail.	As the trail.	Logged in the key owner's account and in the caller's, so the bank's trail holds calls made from account `777788889999`.	As the trail.	The attacker's own account's record of the same calls is not ours to read.
Loan platform application and load-balancer logs	`wf-prod-lending` web and application tier.	90 days (bank setting).	S3 and a log group.	Hashed on sealing (`EVD-018`).	None found in the window copied. Host-level logs are not collected.

The log sources, part 3 of 3.

Source	Coverage	Retention	Delivery	Integrity	Gap
Jenkins controller logs	The controller in `wf-tools`: application, audit, and proxy logs.	Rotated weekly; eight weeks kept on the host.	On the host.	Hashed on sealing (`EVD-012`).	No host image. Nothing outside the log files.
S3 Inventory	The imaging archive, daily.	30 days.	S3, inventory bucket in `wf-prod-imaging`.	The July 7 report, the restore job completion reports, and the verification queries are hashed (`EVD-020`).	A listing of objects and keys, not of who read them.
Interceptor	Sessions followed from the seed key since 02:20 on July 4.	For the engagement.	Reads the trail from `wf-log-archive`.	The case database is hashed (`EVD-022`).	A watch, not a log: it holds only what the trail held.
Flow logs and DNS query logs	Configuration is in `EVD-027`.	Not read in week 1.	Not read in week 1.	Not collected.	Not collected, because no week-1 question needed them.

The preservation record

27 items are preserved as of July 17, 14:30 EDT, and every one was re-verified at 14:30 EDT on July 17: all hashes matched. Preservation began at 03:12 on July 4, when the evidence account `wf-ir-forensics` was created. The first item was sealed at 04:02 EDT; the 24 items sealed through containment on July 9 are the Response's, and the 3 sealed in week 1 are the Investigation's.

The evidence sits in `wf-ir-evidence` in its own account, behind a deny-all policy with one exempt role, the bank's custodian role, S3 Object Lock in compliance mode for 7 years, a legal hold on every object, a separate key the bank administers, and access logging. Each item is one sealed archive, and the SHA-256 below is the hash of that archive as stored. The custodian is Imani Castell; the collector of each item is named in the register. The week-1 additions are the trail history before the incident window (EVD-025), the estate configuration (EVD-026), and the network and log-source configuration (EVD-027), which underlie this report's maps.

The preservation record (EVD-001 to EVD-008).

ID	What	Sealed (EDT)	SHA-256	Lock
EVD-001	The attacker's lifecycle rule on the imaging bucket, captured before removal	July 4, 04:02	`6ab17b15e25d463db2dbbb246cbb99e0a46cb6c91954c87d2ced9084f7b11232`	compliance, hold
EVD-002	Ransom note in the imaging archive bucket, with object metadata	July 4, 04:09	`de415b24095cdbb614b6a7b8652762069bd72cc88022d8e44a7f8e8266f2265d`	compliance, hold
EVD-003	Ransom note in the data lake bucket, with object metadata	July 4, 04:12	`1cb44b7976a154e6b82d0bf942b10efdbbf8b2195b859112d8e831dec88ada47`	compliance, hold
EVD-004	Ransom note in the lending documents bucket, with object metadata	July 4, 04:15	`6bab9ef7668b31adad451193ab1a14e2ff304d08fb332f39f22728871743a0d8`	compliance, hold
EVD-005	GuardDuty and Security Hub exports	July 4, 04:24	`b15510f61f5e7ef5e118152b25d4e725c9132f833154a76f43149f5ef69404ea`	compliance, hold
EVD-006	The service control policy and resource control policy as attached	July 4, 04:38	`33ce25d3b3d28f3defd4036979bcfb0e9a999c8b8dd13f1360ac28d767e7b5c6`	compliance, hold
EVD-007	Attacker key metadata and policy, prod-lending	July 4, 04:41	`f943f9c9cfd99afe5f414260bfac5d12c1e72ad360a6436503ae536119bad75c`	compliance, hold
EVD-008	Attacker key metadata and policy, prod-imaging	July 4, 04:44	`40ebe4b7395d4de692f0586540b6189c9a45aa6f9f44958f0ad8221593e8afb3`	compliance, hold

The preservation record (EVD-009 to EVD-016).

ID	What	Sealed (EDT)	SHA-256	Lock
EVD-009	Attacker key metadata and policy, prod-data	July 4, 04:47	`4c6b555cb2a67644f8d48dc62a95191fdfa742bde3523a1a2f617c16ad8d2d8b`	compliance, hold
EVD-010	IAM credential reports	July 4, 05:18	`65482590ebe3438d8bb685cdd7b94e98d00b87fb57e7fc8bb7b3992d038f8b63`	compliance, hold
EVD-011	IAM account authorization details	July 4, 05:41	`50eba2b214edb6c7c450240645e70199ce706ab8ac3a631d381f72a604e80cc1`	compliance, hold
EVD-012	Jenkins controller logs	July 4, 06:12	`35ad97db3aef47d3f32d23a1cbd1737a189f765e7cc074b70d61d359f709949c`	compliance, hold
EVD-013	Organization trail log files and digest files, June 29 to July 4	July 4, 06:55	`349748af9e730acf822e3b719f04f934719a2a4e04163f658d623f4234e5df7b`	compliance, hold
EVD-014	AWS Config snapshots and configuration history	July 4, 07:30	`8ee731b7f3862fd6fded4585351e4c81314a75178b96ea2d7c6d7291b90c778c`	compliance, hold
EVD-015	Shared database snapshot copy metadata	July 4, 07:55	`bbd6ab6045a88d7f490b68b83e4efb50a703b889f49f068090c24ba8b6e38f18`	compliance, hold
EVD-016	EBS snapshot inventory and Recycle Bin restore records	July 4, 08:35	`f19eaf755e985edb8b8a36b3a78c00fad9363a53c2b5f79e4154753590032bca`	compliance, hold

The preservation record (EVD-017 to EVD-024).

ID	What	Sealed (EDT)	SHA-256	Lock
EVD-017	S3 Batch Operations job record and manifest	July 4, 09:20	`cb904b27616e5a5b7129bf6b50cc3319c5ab2164caec7c3dbf1d3682de6baef5`	compliance, hold
EVD-018	Loan platform application and load-balancer logs	July 5, 10:20	`07f35fc47a2a6258e7512c2cd86ef1d1cf9d69216c4ab702df14816897b41cd5`	compliance, hold
EVD-019	RDS snapshot inventory and Vault Lock record	July 6, 20:10	`6b46c41f269ed9aba6e89bf5bf7856bdd9fda423722e36e9ff450b3c5f761911`	compliance, hold
EVD-020	Restore verification: the 31 job completion reports and the July 7 scheduled inventory	July 7, 15:30	`5c351b64d540d3afc5164cad98623bb46cadec51e53fef83e63aa73390397082`	compliance, hold
EVD-021	The IAM objects the attacker created, captured before deletion	July 8, 09:55	`ef5806c1bc1986fd23b6ee21f4384c8966ee357a23997d8ad18147559b0bed1b`	compliance, hold
EVD-022	Interceptor case database export, as of containment	July 9, 08:58	`cc77bb33ddb2c0ae152fe929262a5025745864730d40582c3cd4b3934e6abb99`	compliance, hold
EVD-023	Organization trail log files and digest files, July 4 to July 9	July 9, 10:12	`2f09c7ba80449b602584db498384c1b1aac9e6ddb01e7a8ae594c8795c2f7860`	compliance, hold
EVD-024	Bridge log	July 9, 10:40	`54764c5d943a0a83ecf036e11a72cb242f0edb1d30b0e1c126f8cf028c7ff578`	compliance, hold

The preservation record (EVD-025 to EVD-027).

ID	What	Sealed (EDT)	SHA-256	Lock
EVD-025	Organization trail history before the incident window, June 1 to June 28	July 13, 11:20	`b30d1be49e21d08ed66d2ea223b5a3d5d5e19d927e08f9d32e2a8313b0126b53`	compliance, hold
EVD-026	Estate configuration export: organization, identities, trust paths, and keys	July 14, 15:10	`981338806a3f2c998cbdfb8ebaba4da7466f1d73349db051db166a7e8c36d945`	compliance, hold
EVD-027	Network exposure and log-source configuration export	July 16, 14:30	`d6ba14fb55e56e5f2dc2456eed4380085b8139b608c6412bc378c3d5609cd6eb`	compliance, hold

What was not preserved. No host image was taken. No flow or DNS log was collected. Nothing outside AWS is in the register. The legacy account trail's configuration was deleted before preservation began.

What week 1 leaves for week 2

Five questions stay open at the end of week 1, and each has a named source. None is answered here.

The open questions and their sources, at the end of week 1.

Question	Where the answer would come from
What each of the three attacker keys encrypted, and whether anything the bank needs was left under them	Trail, key policies, and the restore verification reports and queries (`EVD-007` to `EVD-009`, `EVD-013`, `EVD-020`, `EVD-023`).
What the calls from account `777788889999` on the prod-lending key mean for the database snapshot	The 7 KMS calls in the copy-out burst, and 7 from the account in all, read against the snapshot's attributes and the 137 minutes the share was open (`EVD-015`, `EVD-013`).
Whether any object was read from the imaging archive	Cannot be answered from the logs we hold. Week 2 will say what indirect evidence exists and how far it goes.
Whether the attacker used any principal, account, or credential not yet seen	Every principal in the sealed trail, including the baseline before June 29 (`EVD-025`).
What happened before the first call we know of	The trail history from June 1 (`EVD-025`).

Week 2 is Trace and report, July 20 to July 24. It reads the sealed items, not the live estate, so its findings can be checked against the register.

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.