

Vantalect

AWS INCIDENT RESPONSE · SAMPLE DELIVERABLE

Chain-of-Custody Log (at Containment)

DISTRIBUTION: COUNSEL ONLY

Day 6: Evidence at containment · 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

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 limits 2

The evidence at containment 3

How evidence was collected and sealed 4

The evidence account's controls 5

The register 8

- What each item is 8
- How and when each item was collected 11
- Hash and lock 14
- Transfers 17

Integrity re-verification 25

What the register does not hold 25

Counsel's file: counts the bank ran 27

Notes on individual items 28

Decisions for counsel 33

Notice 34

Scope and limits

This log records every item of evidence that Vantalect and Wrenfield Bank sealed between July 4, 04:02 EDT and July 9, 10:40 EDT, as of July 9, 12:20 EDT on Thursday, July 9, 2026, and what has been done to protect each item since. It exists so that counsel can show where each item came from, who held it, and that it has not changed. It is written for Diane Whitcombe of Tessaly & Brook LLP, and for no one else without counsel's decision.

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 log goes to Diane Whitcombe alone. Counsel forwards it, to whom counsel decides, and keeps the distribution record. Vantalect keeps a record of its own delivery to counsel and of nothing after that.

This log does not say what the evidence shows. It says what exists and that it is intact. The incident's account of events is in the situation reports, and the Investigation, if the bank engages it, will state what the evidence supports. The log makes no legal determination: whether an item will be admissible, whether privilege applies, and what the bank must keep are for counsel to decide.

The log is as of containment, which Mireille Danvers declared in writing at 09:00 EDT on Thursday, July 9. Evidence that the Investigation would collect later is not here, and a final log would replace this one.

The evidence at containment

24 items are sealed in the evidence account, and every one was re-verified at 12:20 EDT on July 9: all hashes matched. The items fall into the groups below. Each is in the register that follows, with its hash, its storage key, and every hand it passed through.

The sealed items at containment, by group.

Group	ItemsItem IDs
Case records	2EVD-022, EVD-024
Data stores	6EVD-001, EVD-015, EVD-016, EVD-017, EVD-019, EVD-020
Identity	3EVD-010, EVD-011, EVD-021
Keys	3EVD-007, EVD-008, EVD-009
Organization trail	2EVD-013, EVD-023
Platform logs	2EVD-012, EVD-018
Policies	1EVD-006
Ransom notes	3EVD-002, EVD-003, EVD-004
Security services	2EVD-005, EVD-014

Three facts about what these items cover.

- **The trail is held in two copies, split by delivery time.** EVD-013 holds the files delivered June 29 00:00 EDT to July 4 04:00 EDT (June 29 04:00 to July 4 08:00 UTC), and EVD-023 the files delivered July 4 04:00 EDT to July 9 09:00 EDT (July 4 08:00 to July 9 13:00 UTC). Each file is in exactly one copy. CloudTrail can deliver a file long after the events in it, so the second copy may hold events from before 04:00 on July 4; the verification output lists any such late file. Digest validation was run over both copies as one set and reported no invalid file. The window before June 29 is not yet in the register.
- **The three attacker keys are in the bank's own accounts, and the shared snapshot's attributes are sealed too.** The keys' policies, grants, and metadata are sealed (EVD-007, EVD-008, EVD-009), and the snapshot attributes (EVD-015). Both were read at about 02:03 on July 4, before the bank's changes at 02:08 to 02:10. The calls from account 777788889999 on the prod-lending key are in the trail, because KMS logs a cross-account call in the key owner's account too.
- **Three ransom notes are sealed, but only two are in the trail.** The notes in the imaging archive and the data lake were written at July 3, 23:30 EDT and are trail events. The lending documents bucket has no data events, so its note (EVD-004) rests on the object's own metadata and the bucket listing.

How evidence was collected and sealed

Every item followed the same five steps, and an item that missed one is not in the register.

The five handling steps.

Step	What was done
Read-only acquisition	Every source was read through the incident role `VantalectIncidentResponse` (or, for the bank's own log files, copied by the named bank collector). Nothing was written to a source system to collect from it.
One sealed archive per item	An item is one archive (`.tar.zst`) with a manifest that lists each file and its SHA-256. The register's SHA-256 is the hash of the archive.
Hash twice, by two people	The collector hashes the archive. The custodian, Imani Castell, deposits it in `wf-ir-evidence` and recomputes the hash from the stored object. An item is not sealed until the two values match.
Lock and hold	On deposit the object is locked in compliance mode for the period counsel chose at activation (given in the controls below), which no one, not even the bank's administrators, can shorten, and given a legal hold, which only the custodian's role can release, and only on counsel's written instruction.
Working copies stay separate	Vantalect's analysis uses working copies, grouped in sets (`WCS-01` to `WCS-05` at containment). A working copy is never the evidence: the sealed object is. Vantalect deletes none of them unless counsel instructs it to in writing.

What the SHA-256 is. It is the hash of the sealed archive as stored, 64 hexadecimal characters. Re-computing it from the stored object and getting the same value shows that the archive has not changed since it was sealed. The hash does not show that the contents were correct when collected; the collection method, the collector, and the time are what show that.

Times. Every time in this log is Eastern Daylight Time (EDT, UTC-4). Trail windows are also given in UTC where an investigator will match them against a log file.

The evidence account's controls

The evidence sits in its own account, `wf-ir-forensics` (`584729107701`), in the Incident OU, behind the controls below. The account was created at 03:12:08 EDT (`EV-00648`) and moved into the OU at 03:14:40 EDT. Evidence preservation began there. The deny-all policy is set in the management account, so only that account can lift it.

The evidence account's controls, all in place before the first item was sealed at 04:02 EDT.

Control	Setting	In place
Service control policy	`wf-evidence-deny-all` (`p-wrnfevid00001`) on the Incident OU: deny all actions except the custodian's role	July 4, 03:52 EDT
The one exempt role	`wf-evidence-custodian` (the bank; custodian Imani Castell). Every deposit was made through it	July 4, 03:52 EDT
Vantalect's access	Vantalect holds no role in this account. Its staff take part in each deposit and check in a session the custodian runs	July 4, 03:52 EDT
S3 Object Lock	Bucket `wf-ir-evidence`: compliance mode, default retention 7 years, the period counsel chose (`EV-00656`, `EV-00657`)	July 4, 03:41 EDT
Legal hold	Set on every object at deposit; only `wf-evidence-custodian` can release it, on counsel's written instruction	At each sealing
Separate key	`alias/wf-ir-evidence`, origin `AWS_KMS`, created in this account and administered by the bank. Vantalect holds no role in the account, so it cannot change the key's policy or schedule its deletion	July 4, 03:46 EDT
Access logging	S3 server access logging to a separate log bucket in `wf-ir-forensics` (server access logging needs the log bucket in the same account and Region as the logged bucket; the bank can replicate those logs to `wf-log-archive`); every management call in the account is also in the organization trail	July 4, 03:56 EDT

What the role can do. `wf-evidence-custodian` can read and write in the bucket, set or release a legal hold on counsel's written instruction, and administer the key. The custodian made every deposit; Vantalect's staff hand over each archive and watch the hash recomputed from the stored object (the transfer record below names both parties each time). The organization's default `OrganizationAccountAccessRole` created the bucket and then fell under the deny-all policy. Neither Vantalect nor the bank's administrators can delete a locked object or shorten its retention; compliance mode allows neither, even for the organization's management account.

What this does not protect against. The controls stop deletion and alteration in the account. They do not stop an authorized custodian from releasing a legal hold or stop the 7-year retention from expiring, and they do not protect the working copies, which Vantalect holds separately.

The lock period is counsel's choice, and no one can shorten it. Counsel chose the legal hold and the lock period at activation (00:52 EDT on July 4), before the bucket default was set at 03:41. An existing object version's compliance-mode retain-until date cannot be shortened. The bucket

default may be changed for future versions, without reducing retention already applied to sealed versions. Counsel to decide whether a compliance lock of this length on items that may hold personal information in log files and exports is consistent with the bank's disposal and data-minimization obligations, including 23 NYCRR 500.13(b), which calls for policies and procedures for the secure disposal on a periodic basis of nonpublic information that is no longer necessary for business operations or other legitimate business purposes, except where the information is required to be retained by law or regulation or targeted disposal is not reasonably feasible. Vantalect makes no determination that it applies. The lock period was set before the first deposit and cannot be shortened for the items already sealed.

The register

The register lists 24 items in the order they were sealed. Four groups of tables follow: what each item is and where it came from, how and when it was collected and sealed, its hash and lock, and then every transfer. The hash is the first line of authentication; the transfer record is the second. All times are EDT.

What each item is

What each item is and where it came from (EVD-001 to EVD-008).

ID	Item	Source account	Source resource
EVD-001	The attacker's lifecycle rule on the imaging bucket, captured before removal	wf-prod-imaging	s3://wf-imaging-archive-prod (lifecycle configuration)
EVD-002	Ransom note in the imaging archive bucket, with object metadata	wf-prod-imaging	s3://wf-imaging-archive-prod/RESTORE-INSTRUCTIONS.txt
EVD-003	Ransom note in the data lake bucket, with object metadata	wf-prod-data	s3://wf-datalake-prod/RESTORE-INSTRUCTIONS.txt
EVD-004	Ransom note in the lending documents bucket, with object metadata	wf-prod-lending	s3://wf-lending-docs-prod/RESTORE-INSTRUCTIONS.txt
EVD-005	GuardDuty and Security Hub exports	wf-audit	GuardDuty detector and Security Hub (delegated administrator account)
EVD-006	The service control policy and resource control policy as attached	wf-management	AWS Organizations policies and their attachments
EVD-007	Attacker key metadata and policy, prod-lending	wf-prod-lending	arn:aws:kms:us-east-1:584729104402:key/b9885f41-4ff8-5cbf-9f54-7753a6180289
EVD-008	Attacker key metadata and policy, prod-imaging	wf-prod-imaging	arn:aws:kms:us-east-1:584729104415:key/6d9bd1af-48a0-5150-b619-9ab79ca2b680

What each item is and where it came from (EVD-009 to EVD-016).

ID	Item	Source account	Source resource
EVD-009	Attacker key metadata and policy, prod-data	wf-prod-data	arn:aws:kms:us-east-1:584729104423:key/33767b29-2aaa-5253-83bf-0d1d670c1e43
EVD-010	IAM credential reports	20 pre-existing accounts	IAM credential report, 20 accounts
EVD-011	IAM account authorization details	20 pre-existing accounts	IAM account authorization details, 20 accounts
EVD-012	Jenkins controller logs	wf-tools	Jenkins controller, EC2 instance in wf-tools (log files)
EVD-013	Organization trail log files and digest files, June 29 to July 4	wf-log-archive	s3://wf-org-trail-logs (organization trail bucket)
EVD-014	AWS Config snapshots and configuration history	wf-audit	Config aggregator `wf-org-aggregator`
EVD-015	Shared database snapshot copy metadata	wf-prod-lending	rds snapshots `wf-los-prod-manual-20260703-2122` and `wf-los-prod-bk-20260703`
EVD-016	EBS snapshot inventory and Recycle Bin restore records	wf-prod-lending and wf-prod-data	EBS snapshots in wf-prod-lending and wf-prod-data; Recycle Bin rule

What each item is and where it came from (EVD-017 to EVD-024).

ID	Item	Source account	Source resource
EVD-017	S3 Batch Operations job record and manifest	wf-prod-imaging	s3 control job in wf-prod-imaging; manifest in the imaging inventory bucket
EVD-018	Loan platform application and load-balancer logs	wf-prod-lending	Loan origination web and application tier; ALB access logs bucket
EVD-019	RDS snapshot inventory and Vault Lock record	wf-prod-lending, wf-backup, and wf-recovery-vault	RDS snapshots in wf-prod-lending, wf-backup, and wf-recovery-vault
EVD-020	Restore verification: the 31 job completion reports and the July 7 scheduled inventory	wf-prod-imaging	s3://wf-imaging-archive-prod-inventory (inventory and job reports)
EVD-021	The IAM objects the attacker created, captured before deletion	wf-prod-data, wf-prod-lending, and wf-prod-imaging	IAM objects in wf-prod-data, wf-prod-lending, and wf-prod-imaging
EVD-022	Pursuit case database export, as of containment	wf-audit	Pursuit case database (wf-audit)
EVD-023	Organization trail log files and digest files, July 4 to July 9	wf-log-archive	s3://wf-org-trail-logs (organization trail bucket)
EVD-024	Bridge log	Outside AWS (Vantalect bridge record)	Bridge log (text and attachments), kept outside the AWS accounts

How and when each item was collected

How and when each item was collected and sealed (EVD-001 to EVD-008).

ID	Collection method	Collector	Source window	Collected (EDT)	Sealed (EDT)
EVD-001	CLI output saved before removal	Imani Castell	Configuration as of 01:34 EDT July 4	July 4, 01:34	July 4, 04:02
EVD-002	Object copy and metadata read	Charles Sieg	Object as found at 04:05 EDT July 4	July 4, 04:05	July 4, 04:09
EVD-003	Object copy and metadata read	Charles Sieg	Object as found at 04:10 EDT July 4	July 4, 04:10	July 4, 04:12
EVD-004	Object copy and metadata read	Charles Sieg	Object as found at 04:13 EDT July 4	July 4, 04:13	July 4, 04:15
EVD-005	Service API export, JSON	Charles Sieg	June 29 00:00 to July 4 04:20 EDT	July 4, 04:16	July 4, 04:24
EVD-006	Organizations API read	Charles Sieg	As attached at 04:35 EDT July 4	July 4, 04:35	July 4, 04:38
EVD-007	KMS API read	Charles Sieg	Key policy and grants at 02:03:40 and 02:04:30 EDT July 4 (before the 02:09 change); key as found at 04:38 EDT	July 4, 02:03	July 4, 04:41
EVD-008	KMS API read	Charles Sieg	Key policy and grants at 02:03:55 and 02:04:45 EDT July 4 (before the 02:09 change); key as found at 04:42 EDT	July 4, 02:03	July 4, 04:44

How and when each item was collected and sealed (EVD-009 to EVD-016).

ID	Collection method	Collector	Source window	Collected (EDT)	Sealed (EDT)
EVD-009	KMS API read	Charles Sieg	Key policy and grants at 02:04:10 and 02:05:00 EDT July 4 (before the 02:09 change); key as found at 04:45 EDT	July 4, 02:04	July 4, 04:47
EVD-010	Credential report per account	Charles Sieg	As generated 04:50 to 05:15 EDT July 4	July 4, 04:50	July 4, 05:18
EVD-011	Authorization details per account	Charles Sieg	As read 05:20 to 05:38 EDT July 4	July 4, 05:20	July 4, 05:41
EVD-012	Log files copied from host	Owen Tribble	June 22 00:00 to July 4 05:30 EDT	July 4, 05:35	July 4, 06:12
EVD-013	Bucket sync, hash manifest	Charles Sieg	Files delivered June 29 00:00 EDT to July 4 04:00 EDT (June 29 04:00 to July 4 08:00 UTC)	July 4, 05:50	July 4, 06:55
EVD-014	Aggregator snapshot query and per-account configuration history calls, JSON	Charles Sieg	Snapshot at 07:05 EDT July 4; history June 29 to July 4	July 4, 07:05	July 4, 07:30
EVD-015	RDS API read, metadata only	Charles Sieg	Attributes as read at 02:03 EDT July 4 (before the share was removed); metadata as read at 07:40 EDT	July 4, 02:03	July 4, 07:55
EVD-016	EC2 API read, JSON	Charles Sieg	Inventory as read 07:50 to 08:20 EDT July 4	July 4, 08:20	July 4, 08:35

How and when each item was collected and sealed (EVD-017 to EVD-024).

ID	Collection method	Collector	Source window	Collected (EDT)	Sealed (EDT)
EVD-017	S3 Control API read	Charles Sieg	Job as of its cancellation at 01:28 EDT July 4	July 4, 08:55	July 4, 09:20
EVD-018	Log objects copied	Imani Castell	June 22 00:00 to July 4 01:50 EDT	July 5, 09:40	July 5, 10:20
EVD-019	RDS and Backup API read	Imani Castell	As read 19:40 EDT July 6	July 6, 19:40	July 6, 20:10
EVD-020	Report files copied	Imani Castell	Completion reports of the 31 restore jobs (July 5 to July 7) and the scheduled inventory delivered July 7; the two queries ran at 13:52 and 13:55 EDT on July 7	July 7, 14:10	July 7, 15:30
EVD-021	IAM API read, no secrets	Charles Sieg	As read 09:30 to 09:52 EDT July 8	July 8, 09:30	July 8, 09:55
EVD-022	Pursuit export	Charles Sieg	Case database as of 08:40 EDT July 9	July 9, 08:40	July 9, 08:58
EVD-023	Bucket sync, hash manifest	Charles Sieg	Files delivered July 4 04:00 EDT to July 9 09:00 EDT (July 4 08:00 to July 9 13:00 UTC)	July 9, 09:20	July 9, 10:12
EVD-024	Text export	Charles Sieg	00:58 EDT July 4 to 09:00 EDT July 9	July 9, 10:20	July 9, 10:40

Hash and lock

Each item's SHA-256, storage key, and lock (EVD-001 to EVD-008).

ID	SHA-256	Storage key	Lock	Retain until
EVD-001	6ab17b15e25d463db2dbbb246cbb99e0a46cb6c91954c87d2ced9084f7b11232	s3://wf-ir-evidence/data-stores/EVD-001.tar.zst	compliance, hold	July 4, 2033
EVD-002	de415b24095cdbb614b6a7b8652762069bd72cc88022d8e44a7f8e8266f2265d	s3://wf-ir-evidence/ransom-notes/EVD-002.tar.zst	compliance, hold	July 4, 2033
EVD-003	1cb44b7976a154e6b82d0bf942b10efdbbf8b2195b859112d8e831dec88ada47	s3://wf-ir-evidence/ransom-notes/EVD-003.tar.zst	compliance, hold	July 4, 2033
EVD-004	6bab9ef7668b31adad451193ab1a14e2ff304d08fb332f39f22728871743a0d8	s3://wf-ir-evidence/ransom-notes/EVD-004.tar.zst	compliance, hold	July 4, 2033
EVD-005	b15510f61f5e7ef5e118152b25d4e725c9132f833154a76f43149f5ef69404ea	s3://wf-ir-evidence/security-services/EVD-005.tar.zst	compliance, hold	July 4, 2033
EVD-006	33ce25d3b3d28f3defd4036979bcfb0e9a999c8b8dd13f1360ac28d767e7b5c6	s3://wf-ir-evidence/policies/EVD-006.tar.zst	compliance, hold	July 4, 2033
EVD-007	f943f9c9cfd99afe5f414260bfac5d12c1e72ad360a6436503ae536119bad75c	s3://wf-ir-evidence/keys/EVD-007.tar.zst	compliance, hold	July 4, 2033
EVD-008	40ebe4b7395d4de692f0586540b6189c9a45aa6f9f44958f0ad8221593e8afb3	s3://wf-ir-evidence/keys/EVD-008.tar.zst	compliance, hold	July 4, 2033

Each item's SHA-256, storage key, and lock (EVD-009 to EVD-016).

ID	SHA-256	Storage key	Lock	Retain until
EVD-009	4c6b555cb2a67644f8d48dc62a95191fdfa742bde3523a1a2f617c16ad8d2d8b	s3://wf-ir-evidence/keys/EVD-009.tar.zst	compliance, hold	July 4, 2033
EVD-010	65482590ebe3438d8bb685cdd7b94e98d00b87fb57e7fc8bb7b3992d038f8b63	s3://wf-ir-evidence/identity/EVD-010.tar.zst	compliance, hold	July 4, 2033
EVD-011	50eba2b214edb6c7c450240645e70199ce706ab8ac3a631d381f72a604e80cc1	s3://wf-ir-evidence/identity/EVD-011.tar.zst	compliance, hold	July 4, 2033
EVD-012	35ad97db3aef47d3f32d23a1cbd1737a189f765e7cc074b70d61d359f709949c	s3://wf-ir-evidence/platform-logs/EVD-012.tar.zst	compliance, hold	July 4, 2033
EVD-013	349748af9e730acf822e3b719f04f934719a2a4e04163f658d623f4234e5df7b	s3://wf-ir-evidence/organization-trail/EVD-013.tar.zst	compliance, hold	July 4, 2033
EVD-014	8ee731b7f3862fd6fded4585351e4c81314a75178b96ea2d7c6d7291b90c778c	s3://wf-ir-evidence/security-services/EVD-014.tar.zst	compliance, hold	July 4, 2033
EVD-015	bbd6ab6045a88d7f490b68b83e4efb50a703b889f49f068090c24ba8b6e38f18	s3://wf-ir-evidence/data-stores/EVD-015.tar.zst	compliance, hold	July 4, 2033
EVD-016	f19eaf755e985edb8b8a36b3a78c00fad9363a53c2b5f79e4154753590032bca	s3://wf-ir-evidence/data-stores/EVD-016.tar.zst	compliance, hold	July 4, 2033

Each item's SHA-256, storage key, and lock (EVD-017 to EVD-024).

ID	SHA-256	Storage key	Lock	Retain until
EVD-017	cb904b27616e5a5b7129bf6b50cc3319c5ab2164caec7c3dbf1d3682de6baef5	s3://wf-ir-evidence/data-stores/EVD-017.tar.zst	compliance, hold	July 4, 2033
EVD-018	07f35fc47a2a6258e7512c2cd86ef1d1cf9d69216c4ab702df14816897b41cd5	s3://wf-ir-evidence/platform-logs/EVD-018.tar.zst	compliance, hold	July 5, 2033
EVD-019	6b46c41f269ed9aba6e89bf5bf7856bdd9fda423722e36e9ff450b3c5f761911	s3://wf-ir-evidence/data-stores/EVD-019.tar.zst	compliance, hold	July 6, 2033
EVD-020	5c351b64d540d3afc5164cad98623bb46cadec51e53fef83e63aa73390397082	s3://wf-ir-evidence/data-stores/EVD-020.tar.zst	compliance, hold	July 7, 2033
EVD-021	ef5806c1bc1986fd23b6ee21f4384c8966ee357a23997d8ad18147559b0bed1b	s3://wf-ir-evidence/identity/EVD-021.tar.zst	compliance, hold	July 8, 2033
EVD-022	cc77bb33ddb2c0ae152fe929262a5025745864730d40582c3cd4b3934e6abb99	s3://wf-ir-evidence/case-records/EVD-022.tar.zst	compliance, hold	July 9, 2033
EVD-023	2f09c7ba80449b602584db498384c1b1aac9e6ddb01e7a8ae594c8795c2f7860	s3://wf-ir-evidence/organization-trail/EVD-023.tar.zst	compliance, hold	July 9, 2033
EVD-024	54764c5d943a0a83ecf036e11a72cb242f0edb1d30b0e1c126f8cf028c7ff578	s3://wf-ir-evidence/case-records/EVD-024.tar.zst	compliance, hold	July 9, 2033

Transfers

Every transfer names both parties and what was checked. A transfer is any change of hands: from the source to the collector, from a collector to Vantalect for hashing, and from Vantalect to the custodian, Imani Castell. No transfer to counsel or anyone else has yet happened.

Transfers, part 1 of 8 (EVD-001 to EVD-004).

ID	Time (EDT)	From	To	What and what was checked
EVD-001	July 4, 01:34	Wrenfield, wf-prod-imaging (owner Rafael Quintero)	Imani Castell	Collected read-only: CLI output saved before removal.
EVD-001	July 4, 03:58	Imani Castell	Charles Sieg	Handed over for hashing and registration; SHA-256 computed.
EVD-001	July 4, 04:02	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-002	July 4, 04:05	Wrenfield, wf-prod-imaging (owner Rafael Quintero)	Charles Sieg	Collected read-only: object copy and metadata read.
EVD-002	July 4, 04:09	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-003	July 4, 04:10	Wrenfield, wf-prod-data (owner Rafael Quintero)	Charles Sieg	Collected read-only: object copy and metadata read.
EVD-003	July 4, 04:12	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-004	July 4, 04:13	Wrenfield, wf-prod-lending (owner Lucía Brandt)	Charles Sieg	Collected read-only: object copy and metadata read.

Transfers, part 2 of 8 (EVD-004 to EVD-007).

ID	Time (EDT)	From	To	What and what was checked
EVD-004	July 4, 04:15	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-005	July 4, 04:16	Wrenfield, wf-audit (owner Mireille Danvers)	Charles Sieg	Collected read-only: service API export, JSON.
EVD-005	July 4, 04:24	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-006	July 4, 04:35	Wrenfield, wf-management (owner Imani Castell)	Charles Sieg	Collected read-only: Organizations API read.
EVD-006	July 4, 04:38	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-007	July 4, 02:03	Wrenfield, wf-prod-lending (owner Lucía Brandt)	Charles Sieg	Collected read-only before the 02:09 policy change: key policy and grants.
EVD-007	July 4, 04:38	Wrenfield, wf-prod-lending (owner Lucía Brandt)	Charles Sieg	Collected read-only again after the change: key metadata, policy, grants, and aliases.
EVD-007	July 4, 04:41	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.

Transfers, part 3 of 8 (EVD-008 to EVD-010).

ID	Time (EDT)	From	To	What and what was checked
EVD-008	July 4, 02:03	Wrenfield, wf-prod-imaging (owner Rafael Quintero)	Charles Sieg	Collected read-only before the 02:09 policy change: key policy and grants.
EVD-008	July 4, 04:42	Wrenfield, wf-prod-imaging (owner Rafael Quintero)	Charles Sieg	Collected read-only again after the change: key metadata, policy, grants, and aliases.
EVD-008	July 4, 04:44	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-009	July 4, 02:04	Wrenfield, wf-prod-data (owner Rafael Quintero)	Charles Sieg	Collected read-only before the 02:09 policy change: key policy and grants.
EVD-009	July 4, 04:45	Wrenfield, wf-prod-data (owner Rafael Quintero)	Charles Sieg	Collected read-only again after the change: key metadata, policy, grants, and aliases.
EVD-009	July 4, 04:47	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-010	July 4, 04:50	Wrenfield, wf-management (owner Imani Castell)	Charles Sieg	Collected read-only: credential report per account.
EVD-010	July 4, 05:18	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.

Transfers, part 4 of 8 (EVD-011 to EVD-014).

ID	Time (EDT)	From	To	What and what was checked
EVD-011	July 4, 05:20	Wrenfield, wf-management (owner Imani Castell)	Charles Sieg	Collected read-only: authorization details per account.
EVD-011	July 4, 05:41	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-012	July 4, 05:35	Wrenfield, wf-tools Jenkins controller (owner Imani Castell)	Owen Tribble	Collected read-only: log files copied from host.
EVD-012	July 4, 05:52	Owen Tribble	Charles Sieg	Handed over for hashing and registration; SHA-256 computed.
EVD-012	July 4, 06:12	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-013	July 4, 05:50	Wrenfield, wf-log-archive (owner Mireille Danvers)	Charles Sieg	Collected read-only: bucket sync, hash manifest.
EVD-013	July 4, 06:55	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-014	July 4, 07:05	Wrenfield, wf-audit (owner Mireille Danvers)	Charles Sieg	Collected read-only: the aggregator snapshot query (point in time) and, separately, one `get-resource-config-history` call per resource in each of the three attacked accounts for June 29 to July 4, JSON, all sealed in the item under one hash.

Transfers, part 5 of 8 (EVD-014 to EVD-017).

ID	Time (EDT)	From	To	What and what was checked
EVD-014	July 4, 07:30	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-015	July 4, 02:03	Wrenfield, wf-prod-lending (owner Lucía Brandt)	Charles Sieg	Collected read-only before the share was removed: snapshot attributes, metadata only.
EVD-015	July 4, 07:40	Wrenfield, wf-prod-lending (owner Lucía Brandt)	Charles Sieg	Collected read-only again after the removal: snapshot metadata and attributes, metadata only.
EVD-015	July 4, 07:55	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-016	July 4, 08:20	Wrenfield, wf-prod-lending (owner Lucía Brandt)	Charles Sieg	Collected read-only: ec2 API read, JSON.
EVD-016	July 4, 08:35	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-017	July 4, 08:55	Wrenfield, wf-prod-imaging (owner Rafael Quintero)	Charles Sieg	Collected read-only: S3 control API read.
EVD-017	July 4, 09:20	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.

Transfers, part 6 of 8 (EVD-018 to EVD-020).

ID	Time (EDT)	From	To	What and what was checked
EVD-018	July 5, 09:40	Wrenfield, wf-prod-lending (owner Lucía Brandt)	Imani Castell	Collected read-only: log objects copied.
EVD-018	July 5, 10:05	Imani Castell	Charles Sieg	Handed over for hashing and registration; SHA-256 computed.
EVD-018	July 5, 10:20	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-019	July 6, 19:40	Wrenfield, wf-prod-lending (owner Lucía Brandt)	Imani Castell	Collected read-only: RDS and backup API read.
EVD-019	July 6, 19:55	Imani Castell	Charles Sieg	Handed over for hashing and registration; SHA-256 computed.
EVD-019	July 6, 20:10	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-020	July 7, 14:10	Wrenfield, wf-prod-imaging (owner Rafael Quintero)	Imani Castell	Collected read-only: report files copied.
EVD-020	July 7, 15:05	Imani Castell	Charles Sieg	Handed over for hashing and registration; SHA-256 computed.

Transfers, part 7 of 8 (EVD-020 to EVD-024).

ID	Time (EDT)	From	To	What and what was checked
EVD-020	July 7, 15:30	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-021	July 8, 09:30	Wrenfield, wf-prod-data (owner Rafael Quintero)	Charles Sieg	Collected read-only: IAM API read, no secrets.
EVD-021	July 8, 09:55	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-022	July 9, 08:40	Vantalect Pursuit, wf-audit (owner Mireille Danvers)	Charles Sieg	Collected read-only: Pursuit export.
EVD-022	July 9, 08:58	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-023	July 9, 09:20	Wrenfield, wf-log-archive (owner Mireille Danvers)	Charles Sieg	Collected read-only: bucket sync, hash manifest.
EVD-023	July 9, 10:12	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.
EVD-024	July 9, 10:20	Wrenfield incident bridge (sponsor Mireille Danvers)	Charles Sieg	Collected read-only: text export.

Transfers, part 8 of 8 (EVD-024 to EVD-024).

ID	Time (EDT)	From	To	What and what was checked
EVD-024	July 9, 10:40	Charles Sieg	Imani Castell	Received by the custodian and deposited in `wf-ir-evidence`; hash recomputed from the stored object, matched; lock and hold applied.

Integrity re-verification

At 12:20 EDT on Thursday, July 9, Imani Castell (custodian) and Charles Sieg re-verified all 24 items, and all hashes matched. The method was SHA-256 recomputed from each stored object and compared with the register; Object Lock mode and retention read back. The check is repeatable: anyone with read access to the bucket can recompute any hash and compare it with the register.

The July 9 re-verification, as of 12:20 EDT.

Check	Items	Result
Hash recomputed from the stored object and compared with the register	24	all hashes matched
Object Lock mode and retention read back	24	All items in compliance mode, retention 7 years from sealing
Legal hold read back	24	All items held
Trail digest chain validated over the union of the two sealed copies	2	No invalid file (EVD-013, EVD-023)

A hash mismatch would be reported to counsel at once, with the item, the two values, and the time. None has occurred.

What the register does not hold

Eight things are not evidence that Vantalect holds, and counsel should not assume otherwise.

What is not in the register, and why.

What	Why it is not in the register
Object reads from the imaging archive	S3 data events recorded writes only. No log exists to collect, so whether any object was read is unknown.
The lending documents bucket's write log	That bucket has no data events. Its ransom note is evidenced by the object's own metadata (EVD-004), not by a trail record.
Host images of any instance, including the Jenkins controller	None was taken. EVD-012 holds the controller's logs only.
The attacker's own account and infrastructure	Vantalect has no access to account `777788889999`. What it did there is not evidence we hold; only the calls it made into the bank's accounts are.
Devices outside AWS, including any contractor's laptop	Outside AWS and outside Vantalect's access. Securing any such evidence is for counsel.
The database snapshot's data	Only the snapshot's metadata and attributes are collected (EVD-015). Copying the applicants' records into an evidence bucket would widen the exposure, not narrow it.
The 46 EBS snapshot copies in `wf-recovery-vault`	Recovery copies, not preserved evidence. Locked in compliance mode; the lock ends about Monday, July 20, 05:45 EDT.
The 10 RDS snapshot copies in `wf-recovery-vault`	Recovery copies, not evidence, and plain snapshots with no lock of their own.

The vault copies. Each EBS copy was locked with `LockSnapshot` in compliance mode for 14 days with a 72-hour cool-off, Monday, July 6, 05:45 EDT (the calls run to 05:48 EDT). The cool-off ended Thursday, July 9, 05:45 EDT, so the lock now cannot be shortened. The sealed trail shows no extension, and counsel decides whether the copies are kept after the lock ends. The RDS copies rest on the vault OU service control policy, which also denies deletion and key changes to everyone, and keys the bank holds. The weakest link is someone with Organizations rights in the management account who could change that policy.

Object reads from the imaging archive are unknown, and the log says so plainly: the trail recorded writes to the archive and not reads, so there is nothing to collect that would show either way.

Counsel's file: counts the bank ran

The record counts come from the bank's own queries, and they are in counsel's file, not in the register. Vantalect's role cannot read the bank's stored data, so Vantalect ran no count and does not attest to any count. The bank ran each query on its own system of record; the register's EVD-015 holds the snapshot's metadata only. The hash is the one in the bank's transmittal to counsel, and Vantalect has not seen the file. The split by state of residence was not available on July 9.

Counsel's file: counts the bank ran, as of July 9.

Ref	Count	Run on	Run by	Run (EDT)	File and SHA-256
CF-001	412,317 applicant records	the loan origination database `wf-los-prod` in `wf-prod-lending`, the source of the shared snapshot	the bank's lending operations team (owner Lucía Brandt)	July 5, 08:40	`los-applicant-count-20260705.csv` `4c3ad2f01ad231467ef2e8687e0e8bc189b5a93ac5ab0ce30098bb1ca8620f89`

Notes on individual items

Six notes follow, each on items that need context before they are relied on.

Notes on items whose collection time or content needs context.

Item	Note
EVD-001	Captured at 01:34 on July 4, before the evidence account existed (created 03:12), because the bank removed the rule at 01:35. The saved output was held by Imani Castell until it was handed to Vantalect at 03:58 and sealed at 04:02. The rule's text is independently in the trail record `EV-00312`, which the sealed trail copy holds.
EVD-007 to EVD-009	Each item holds two reads. The first, at 02:03 to 02:05 on July 4, took the key policy and grants before the bank's changes at 02:09 (policy) and 02:10 (the lending key's grant). The first reads were held in Vantalect's incident workspace until deposit, because the evidence account did not exist until 03:12. The second, at 04:38 to 04:45, shows the keys after the changes. The captures are of the key policy and metadata as the attacker left them; they are not evidence of what the keys did. The imported key material of the three keys expired at 18:00 on July 7, which put each key in the PendingImport state. The bank's calls to disable the keys on July 8 (10:03:30, 10:03:55, and 10:04:20) were rejected with `KMSInvalidStateException` (`EV-01052`, `EV-01054`, `EV-01056`); those rejected calls are in the trail and no key change succeeded that day. The keys are kept as they are for counsel.
EVD-015	The snapshot attributes were read at 02:03:10, before the bank removed the outside account from the share at 02:08:20 (`EV-00632`), and again at 07:40. Only the first read shows the share as the attacker left it. The snapshot's data was never collected.
EVD-020	The 14:00 reading rests on the 31 restore jobs' completion reports, a canary check (an object written at 13:20 was found in the bucket's S3 Metadata live inventory table by a query at 13:50, so the table covered writes through 13:20, after the rewrite finished at 12:40), and two count queries of that table (13:52 and 13:55), not on the scheduled S3 Inventory report of July 7. S3 Inventory is delivered on a schedule and cannot be run on demand, so that report is provisional: it is a snapshot as of its run and cannot show the bucket after the rewrite finished at 12:40. A later scheduled inventory would confirm inventory and encryption-type coverage, not the KMS key identity (that comes from per-version metadata such as the live table's `kms_key_arn` column); it is not sealed here. The register holds the trail events of the canary query and the two count queries (`EV-01034`, `EV-01035`, `EV-01036`), which show submission, not completion or a zero result, and not their result files. Until the execution metadata, complete result objects, manifests, and hashes are preserved here, the zero is labeled bank-reported; query results not independently preserved.
EVD-021	Captured on July 8 between 09:30 and 09:52, before the deletions at 10:00. The user's access-key record holds no secret, and none was ever collected.

Item	Note
EVD-013 and EVD-023	The two trail copies are split by delivery time at 04:00 EDT on July 4 (S3 key and LastModified), so each file is in exactly one copy. CloudTrail can deliver a file long after its events, so the second copy may hold events from before 04:00; late files, if any, are listed in the verification output. Digest validation was run over both copies as one set. A file delivered after the second copy's 09:00 cut-off on July 9 is in neither.

Each item's full description follows.

EVD-001. The attacker's lifecycle rule on the imaging bucket, captured before removal. The bucket lifecycle configuration as the attacker set it: rule `expire-old-versions`, noncurrent versions expire after 1 day. Set at 21:14 on July 3 (`EV-00312`); removed at 01:35 on July 4 (`EV-00568`). The saved output is the only copy of the rule as it stood.

EVD-002. Ransom note in the imaging archive bucket, with object metadata. `RESTORE-INSTRUCTIONS.txt` written at 23:30 on July 3 (`EV-00518`), encrypted under the attacker's imaging key. The sealed copy holds the object, its version ID, ETag, size, and metadata. The demand and the contact are not reproduced in reports; the contact is withheld.

EVD-003. Ransom note in the data lake bucket, with object metadata. `RESTORE-INSTRUCTIONS.txt` written at 23:30 on July 3 (`EV-00519`), encrypted under the attacker's data key. Object, version ID, ETag, size, and metadata sealed together.

EVD-004. Ransom note in the lending documents bucket, with object metadata. `RESTORE-INSTRUCTIONS.txt` found in the bucket listing, last modified about 23:30 on July 3. This bucket has no data events, so the trail holds no record of the write: the object's own metadata and the listing are the only evidence of it.

EVD-005. GuardDuty and Security Hub exports. Every GuardDuty finding and every Security Hub finding for the organization from June 29 to 04:20 on July 4, including `Persistence:IAMUser/AnomalousBehavior` raised in `wf-audit` at 22:44 on July 3 and its forwarding to the managed security service provider. Both services keep findings for a limited period, so the export is the durable copy.

EVD-006. The service control policy and resource control policy as attached. `wf-incident-containment` (`p-wrnfcontain01`) in both versions (created 01:16, attached to the Workloads OU at 01:22, updated at 02:58), the resource control policy `wf-deny-outside-access` (`p-wrnfrcp00001`, attached at 03:20), and the evidence account's and vault's deny-all policies, each with its list of targets.

EVD-007. Attacker key metadata and policy, prod-lending. Metadata, key policy, and grants of the `alias/wf-backup-2026` key created in `wf-prod-lending` (`EV-00084`): origin `EXTERNAL`, material valid to 2026-07-07T22:00:00Z. Two reads are sealed together. At 02:03:40 and 02:04:30 on

July 4, before the bank changed anything (EV-00626, EV-00629), the policy held the default root statement plus a statement naming account 777788889999. The key carried the one grant recorded at EV-00522; the bank revoked it at 02:10:30 (EV-00636). The bank replaced the policy at 02:09:05 (EV-00633), dropping the outside statement; the later read shows the key after that change. Aliases and key state are included. The key's imported material expired at 18:00 on July 7, which put it in the PendingImport state. The bank's DisableKey on it at 10:03:30 on July 8 was rejected with KMSInvalidStateException (EV-01052); the key was not disabled and is kept as it is for counsel. That rejected call is in the trail and is not part of this item's reads.

EVD-008. Attacker key metadata and policy, prod-imaging. Metadata, key policy, and grants of the alias/wf-backup-2026 key created in wf-prod-imaging (EV-00089): origin EXTERNAL, material valid to 2026-07-07T22:00:00Z. Two reads are sealed together. At 02:03:55 and 02:04:45 on July 4, before the bank changed anything (EV-00627, EV-00630), the policy held the default root statement plus a statement naming account 777788889999. No grant is recorded in the trail for this key. The bank replaced the policy at 02:09:25 (EV-00634), dropping the outside statement; the later read shows the key after that change. Aliases and key state are included. The key's imported material expired at 18:00 on July 7, which put it in the PendingImport state. The bank's DisableKey on it at 10:03:55 on July 8 was rejected with KMSInvalidStateException (EV-01054); the key was not disabled and is kept as it is for counsel. That rejected call is in the trail and is not part of this item's reads.

EVD-009. Attacker key metadata and policy, prod-data. Metadata, key policy, and grants of the alias/wf-backup-2026 key created in wf-prod-data (EV-00093): origin EXTERNAL, material valid to 2026-07-07T22:00:00Z. Two reads are sealed together. At 02:04:10 and 02:05:00 on July 4, before the bank changed anything (EV-00628, EV-00631), the policy held the default root statement plus a statement naming account 777788889999. No grant is recorded in the trail for this key. The bank replaced the policy at 02:09:45 (EV-00635), dropping the outside statement; the later read shows the key after that change. Aliases and key state are included. The key's imported material expired at 18:00 on July 7, which put it in the PendingImport state. The bank's DisableKey on it at 10:04:20 on July 8 was rejected with KMSInvalidStateException (EV-01056); the key was not disabled and is kept as it is for counsel. That rejected call is in the trail and is not part of this item's reads.

EVD-010. IAM credential reports. One credential report for each of the 20 accounts that existed before the response: every IAM user, its access keys with creation and last-use dates, and MFA status. The report for wf-tools holds svc-artifact-sync and its key (created 03/14/2023, never rotated); the report for wf-prod-data holds aws-support-sync.

EVD-011. IAM account authorization details. Every IAM user, group, role, and policy in each of the 20 pre-existing accounts, with trust policies and attached and inline policies, including wf-deploy-pipeline in the ten workload accounts and the three principals the attacker created.

EVD-012. Jenkins controller logs. The controller's application log, its audit-trail log, and its reverse-proxy access log from the `wf-tools` build host, June 22 to July 4. Logs only: no disk or memory image was taken.

EVD-013. Organization trail log files and digest files, June 29 to July 4. Every log file and every digest file the organization trail `wf-org-trail` delivered from 00:00 on June 29 to 04:00 on July 4, selected by delivery time (the S3 key and the object's LastModified time) and not by the time of the events inside: the management events of every account and the write-only S3 data events on the imaging and data-lake buckets. A file delivered after 04:00 that holds events from before 04:00 belongs to the second copy (`EVD-023`), not to this one. CloudTrail log-file validation was run over this copy and `EVD-023` together, so the digest chain is checked across the cut, and no file was reported invalid.

EVD-014. AWS Config snapshots and configuration history. A point-in-time configuration snapshot from the organization aggregator for all accounts, and, from separate `get-resource-config-history` calls in each of the three attacked accounts, the configuration history of their resources for June 29 to July 4. The aggregator query gives aggregated state only, not the history. Config records the resources' state, which the trail does not (for example, the bucket lifecycle rule and the key policies at each change).

EVD-015. Shared database snapshot copy metadata. Metadata of the snapshot `wf-los-prod-manual-20260703-2122` (created 21:22, `EV-00317`) and its attacker-key copy `wf-los-prod-bk-20260703` (`EV-00442`, completed 23:40), and the copy's attributes. The attributes were read at 02:03:10 on July 4 (`EV-00625`), before the bank removed account `777788889999` from the share at 02:08:20 (`EV-00632`); that read shows the share the attacker added at 23:51 (`EV-00520`). The read at 07:40 shows the copy after the removal. The snapshot data itself is not collected.

EVD-016. EBS snapshot inventory and Recycle Bin restore records. The inventory of the 46 EBS snapshots (31 in `wf-prod-lending`, 15 in `wf-prod-data`) before deletion, after deletion, and after restore, with the Recycle Bin retention rule (10 days) and the 46 restore calls at 07:40 and 07:41 (`EV-00673` to `EV-00719`).

EVD-017. S3 Batch Operations job record and manifest. Job `45eb31f1-d889-53b5-ac3d-236b4a64dea8` (created 21:41, `EV-00393`; canceled 01:28, `EV-00565`): the job description, its manifest location and manifest, and its progress counters at cancellation. The attacker created the job with the completion report disabled, so no completion report exists; the counters stand in for it.

EVD-018. Loan platform application and load-balancer logs. The loan origination platform's application logs and its Application Load Balancer access logs, June 22 to July 4 01:50 EDT, when the bank took the platform offline.

EVD-019. RDS snapshot inventory and Vault Lock record. The inventory of the nine month-end manual snapshots (deleted at 22:05 on July 3, restored from `wf-backup`), their copies and the live database snapshot copy in `wf-recovery-vault` (ten RDS copies, plain snapshots with no lock of their own), and the Backup Vault Lock configuration on the vault `wf-recovery` (minimum retention 14 days, changeable for 3 days, then compliance mode) set at 19:30 on July 6 (`EV-00998`). That lock covers one recovery point of the live database. The 46 EBS snapshot copies in the vault are not part of this item or of the register.

EVD-020. Restore verification: the 31 job completion reports and the July 7 scheduled inventory. The evidence for the bank's check of the imaging archive rewrite. It holds the completion reports of the 31 restore slice jobs (each job was created with a report on all tasks, written under `rewrite-reports` in the inventory bucket; the first job is `EV-00737`) and the scheduled S3 Inventory report delivered on July 7 (manifest and data files), kept as provisional. The bank's 14:00 reading, 0 current business-data versions under any attacker key ARN, with the preserved ransom-note versions outside that population (bank-reported; query results not independently preserved), came from two queries run at 13:52 and 13:55 on July 7 against the bucket's S3 Metadata live inventory table (`EV-01035`, `EV-01036`); the trail records both queries, and each was set to write its result under `athena-results` in the inventory bucket. This item holds the two queries' trail events, which show submission and not completion or a zero result, and not their result files; it does not prove that no current object remained under an attacker key. S3 Inventory is a scheduled snapshot that cannot be run on demand, so the July 7 report does not show the bucket after the rewrite finished at 12:40; a later scheduled inventory would confirm inventory and encryption-type coverage, not the KMS key identity, and sits in the bank's inventory bucket, not in this register.

EVD-021. The IAM objects the attacker created, captured before deletion. User `aws-support-sync` (with its attached `AdministratorAccess` and the access key record for `AKIAWRFNEXAMPLE00002`, no secret), role `OrgAccessBackup` with its trust policy naming account `777788889999`, and role `s3-batch-replication` with its trust and permissions. Captured at 09:30 to 09:52 on July 8, before the deletions that began at 10:00 (`EV-01045` to `EV-01051`).

EVD-022. Pursuit case database export, as of containment. The case database of Vantalect's Pursuit watch in `wf-audit` as it stood at containment: the seed key, the sessions followed since 02:20 on July 4 (the 37 `wf-deploy-pipeline` sessions), the principals Pursuit found, and the alerts raised (02:50 and 14:15).

EVD-023. Organization trail log files and digest files, July 4 to July 9. The trail's log and digest files delivered from 04:00 on July 4 to the declaration of containment at 09:00 on July 9, selected by delivery time. This window holds the response itself: every containment action, the Recycle Bin restores, the key material expiry on July 7 at 18:00, and the eradication on July 8. It also holds any

late file, meaning a file delivered after 04:00 whose events are from before 04:00; such files are listed in the verification output, and the method, not a count, is the point. Log-file validation was run over this copy and `EVD-013` as one set, with no file reported invalid.

EVD-024. Bridge log. The incident bridge's running record from 00:58 on July 4 to the declaration of containment at 09:00 on July 9: who joined and when, each decision and who made it, each approval, each notice made, and the clock entries. Kept by Vantalect; the closing entry confirmed by Mireille Danvers.

Decisions for counsel

Five decisions are counsel's, and none of them blocks the Response's close.

- Counsel chose the legal hold and the lock period at activation on July 4. Counsel to say who may release a legal hold, and whether any item is to be released or added.
- Counsel to say whether, and to whom, working copies are handed over, and when. Each handover is logged here as a transfer with both parties and a hash check. Vantalect deletes no working copy unless counsel instructs it to in writing.
- If the bank engages Vantalect for the Investigation, the first week adds the trail history before June 29 and the estate's configuration to this register.
- Counsel to decide whether a compliance lock of this length on items that may hold personal information in log files and exports is consistent with the bank's disposal and data-minimization obligations, including 23 NYCRR 500.13(b), which calls for policies and procedures for the secure disposal on a periodic basis of nonpublic information that is no longer necessary for business operations or other legitimate business purposes, except where the information is required to be retained by law or regulation or targeted disposal is not reasonably feasible. Vantalect makes no determination that it applies. The lock period was set before the first deposit and cannot be shortened for the items already sealed.
- Counsel to decide whether the 46 EBS recovery copies are kept, and how: their lock ends about Monday, July 20, and they are the bank's copies in the bank's vault account.

Vantalect holds working copies of the sealed items in five sets, `WCS-01` to `WCS-05`. They are not evidence. Vantalect deletes none of its working copies unless counsel instructs it to in writing (opt-in). It takes no deletion step on its own schedule, and none once counsel indicates that litigation is reasonably anticipated. If counsel gives that instruction, the sets are listed with their hashes and their destruction is certified against this 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.