Vantalect



AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

Chain-of-Custody Log (Final)

DISTRIBUTION: COUNSEL ONLY

Week 4 of 4: Hand over · prepared for Wrenfield Bancorp, Inc.

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

August 7, 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, limits, and how to read this log 2

The custody record at the close 3

The evidence account's controls 5

What the register does not hold 6

Counsel's file: counts the bank ran 7

The register 7

What each item is 8

How and when each item was collected 12

Hash and lock 16

Transfers 20

Disposition of each item 32

Integrity re-verification 39

Vantalect's working copies 39

Certificate of destruction 40

Counsel's instruction 41

How the sets were destroyed 41

The sets destroyed 41

Attestation 42

Notice 42

Scope, limits, and how to read this log

This is the closing custody record for the evidence in `wf-ir-evidence`, as of 16:25 EDT on Friday, August 7, 2026: 29 items, all intact, all retained, and every working copy Vantalect made destroyed on counsel's written instruction and certified. It adds the items collected after containment to the log delivered on Thursday, July 9, records what was decided about each item, and carries the certificate of destruction in its last section.

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 of Tessaly & Brook LLP 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.

What this log does not do.

- The register is Vantalect's and the bank's record of what was collected and kept. It is not a finding that any item is authentic, complete, or admissible; counsel decides how each item is used.
- Object reads from the imaging archive are unknown, because reads were not logged. No evidence item can show them either way.
- Evidence outside AWS (any contractor's laptop, the bank's own endpoint tools, the core banking service bureau) is not in the register.

How to read it with either engagement. Delivered with the four-week engagement, this log closes on August 7. If an engagement ends with the Investigation alone, the same log closes at the readout instead: it omits every item and working-copy set marked Recovery (EVD-029 and WCS-08), counsel's retention instruction, counsel's destruction instruction, and the destruction certificate carry that closing date, and nothing else in the record changes. The register marks each item with the phase in which it was collected: Response, Investigation, or Recovery.

The custody record at the close

29 items were collected and sealed, 24 in the Response, 4 in the Investigation, and 1 in the Recovery. The last check, at 15:30 EDT on August 7, recomputed every hash from the stored objects, and all hashes matched. No item has been altered, replaced, or removed since it was sealed. No hash has ever failed a check, at the sealing, at any re-verification, or at either handover to counsel.

The register by phase.

Phase	ItemsSealed	Item IDs
Response	24July 4 to July 9	EVD-001 to EVD-024
Investigation	4July 13 to July 22	EVD-025 to EVD-028
Recovery	1August 7	EVD-029

The register by group.

Group	ItemsItem IDs
Case records	4EVD-022, EVD-024, EVD-028, EVD-029
Data stores	6EVD-001, EVD-015, EVD-016, EVD-017, EVD-019, EVD-020
Estate	2EVD-026, EVD-027
Identity	3EVD-010, EVD-011, EVD-021
Keys	3EVD-007, EVD-008, EVD-009
Organization trail	3EVD-013, EVD-023, EVD-025
Platform logs	2EVD-012, EVD-018
Policies	1EVD-006
Ransom notes	3EVD-002, EVD-003, EVD-004
Security services	2EVD-005, EVD-014

What the Investigation and the Recovery added. The Response's 24 items hold the incident as it happened and the response to it. The later items hold what week-one mapping needed and what the later work produced: the trail history before June 29 (EVD-025), the estate's configuration (EVD-026, EVD-027), Interceptor's replay output (EVD-028), and the closure sweep with the seven-day watch (EVD-029).

How the log was built. Every item followed the same steps: read-only acquisition, one sealed archive with a manifest of per-file hashes, a SHA-256 computed by the collector and recomputed by the custodian, Imani Castell, from the stored object, then an Object Lock and a legal hold. A hash is the hash of the archive as stored. It shows that the archive has not changed since it was sealed; the method, the collector, and the time show that the contents were correct when collected.

All times are Eastern Daylight Time (EDT, UTC-4). The archive's windows are also given in UTC where an investigator will match them against a log file.

The evidence account's controls

The evidence is in `wf-ir-forensics` (`584729107701`), in the Incident OU, and the controls that were in place at the first sealing are in place now. The account was created at 03:12:08 EDT (`EV-00648`) on Saturday, July 4, and the first item was sealed at 04:02 EDT. Nothing in the controls was changed during the Investigation or the Recovery. The deny-all policy is set in the management account, so only that account can lift it.

The evidence account's controls, unchanged since July 4.

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 handed over each archive and watched the hash recomputed from the stored object.

What the controls do not protect against. They stop deletion and alteration in the account. They do not stop an authorized custodian from releasing a legal hold, and they do not stop the 7-year retention from expiring. Counsel's instruction of August 6 governs both.

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.

What the register does not hold

Two sets of copies in the recovery vault are not evidence, and Vantalect did not collect them. They are the bank's recovery copies, listed here so no one reads them as preserved evidence.

The recovery copies that are not in the register.

Copies	Status as of August 7
The 46 EBS snapshot copies in `wf-recovery-vault`	Recovery copies, not preserved evidence, and not in the register. Each was locked 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 lock period ended about Monday, July 20, 05:45 EDT, before the date of this log. The sealed trail, which ends Thursday, July 9, shows the lock calls and no extension. We have not read the copies' lock state since, so whether they are still locked is for the bank to state. Counsel decides whether they are kept.
The 10 RDS snapshot copies in `wf-recovery-vault`	Recovery copies, not evidence, and plain snapshots with no lock of their own. They 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.

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; EVD-015 holds the snapshot's metadata only, and its data was never collected. The hash is the one in the bank's transmittal to counsel, and Vantalect has not seen the file. Counsel to decide how the counts are used.

Counsel's file: counts the bank ran.

Ref	Count	Run on	Run by	Run (EDT)	Delivered to	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	the incident bridge, reported at 09:30 and entered in counsel's file, July 5, 09:30	`los-applicant-count-20260705.csv` `4c3ad2f01ad231467ef2e8687e0e8bc189b5a93ac5ab0ce30098bb1ca8620f89`
CF-002	389,904 New York, 15,077 Pennsylvania, 7,336 other	the loan origination database restored from the 21:22 snapshot (`wf-los-vault`, `EV-00954`)	the bank's lending operations team (owner Lucía Brandt)	July 20, 16:40	Diane Whitcombe, July 20, 17:05	`los-applicant-count-by-state-20260720.csv` `ad02f5580e34838229913f18bbbaead2f365c86e8526598042ec3cae231cfb13`

The register

The register lists 29 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, its hash and lock, and every transfer. All times are EDT.

What each item is

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

ID	Phase	Item	Source account	Source resource
EVD-001	Response	The attacker's lifecycle rule on the imaging bucket, captured before removal	wf-prod-imaging	s3://wf-imaging-archive-prod (lifecycle configuration)
EVD-002	Response	Ransom note in the imaging archive bucket, with object metadata	wf-prod-imaging	s3://wf-imaging-archive-prod/RESTORE-INSTRUCTIONS.txt
EVD-003	Response	Ransom note in the data lake bucket, with object metadata	wf-prod-data	s3://wf-datalake-prod/RESTORE-INSTRUCTIONS.txt
EVD-004	Response	Ransom note in the lending documents bucket, with object metadata	wf-prod-lending	s3://wf-lending-docs-prod/RESTORE-INSTRUCTIONS.txt
EVD-005	Response	GuardDuty and Security Hub exports	wf-audit	GuardDuty detector and Security Hub (delegated administrator account)
EVD-006	Response	The service control policy and resource control policy as attached	wf-management	AWS Organizations policies and their attachments
EVD-007	Response	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	Response	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	Phase	Item	Source account	Source resource
EVD-009	Response	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	Response	IAM credential reports	20 pre-existing accounts	IAM credential report, 20 accounts
EVD-011	Response	IAM account authorization details	20 pre-existing accounts	IAM account authorization details, 20 accounts
EVD-012	Response	Jenkins controller logs	wf-tools	Jenkins controller, EC2 instance in wf-tools (log files)
EVD-013	Response	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	Response	AWS Config snapshots and configuration history	wf-audit	Config aggregator `wf-org-aggregator`
EVD-015	Response	Shared database snapshot copy metadata	wf-prod-lending	rds snapshots `wf-los-prod-manual-20260703-2122` and `wf-los-prod-bk-20260703`
EVD-016	Response	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	Phase	Item	Source account	Source resource
EVD-017	Response	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	Response	Loan platform application and load-balancer logs	wf-prod-lending	Loan origination web and application tier; ALB access logs bucket
EVD-019	Response	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	Response	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	Response	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	Response	Interceptor case database export, as of containment	wf-audit	Interceptor case database (wf-audit)
EVD-023	Response	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	Response	Bridge log	Outside AWS (Vantalect bridge record)	Bridge log (text and attachments), kept outside the AWS accounts

What each item is and where it came from (EVD-025 to EVD-029).

ID	Phase	Item	Source account	Source resource
EVD-025	Investigation	Organization trail history before the incident window, June 1 to June 28	wf-log-archive	s3://wf-org-trail-logs (organization trail bucket)
EVD-026	Investigation	Estate configuration export: organization, identities, trust paths, and keys	All 22 accounts	AWS Organizations and IAM and KMS in 22 accounts
EVD-027	Investigation	Network exposure and log-source configuration export	All 22 accounts	EC2, ELB, S3, CloudTrail, GuardDuty, Security Hub, Config, and EventBridge in 22 accounts
EVD-028	Investigation	Interceptor replay output	Vantalect (derived from sealed items)	Interceptor replay output (generated from sealed items)
EVD-029	Recovery	Closure sweep results and seven-day watch record	wf-audit	Closure sweep output and Interceptor watch record (wf-audit)

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	Interceptor 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

How and when each item was collected and sealed (EVD-025 to EVD-029).

ID	Collection method	Collector	Source window	Collected (EDT)	Sealed (EDT)
EVD-025	Bucket sync, hash manifest	Charles Sieg	Files delivered June 1 00:00 EDT to June 29 00:00 EDT	July 13, 09:30	July 13, 11:20
EVD-026	Scripted read-only export	Charles Sieg	As read 09:45 to 15:00 EDT July 14	July 14, 09:45	July 14, 15:10
EVD-027	Scripted read-only export	Charles Sieg	As read 10:00 to 14:20 EDT July 16	July 16, 10:00	July 16, 14:30
EVD-028	Interceptor replay, hash manifest	Charles Sieg	Replay over the items sealed to July 17	July 22, 15:30	July 22, 16:40
EVD-029	Interceptor export, hash manifest	Charles Sieg	Sweep August 3 to August 5; watch July 31 09:00 to August 7 09:00 EDT	August 7, 11:40	August 7, 12:10

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

Each item's SHA-256, storage key, and lock (EVD-025 to EVD-029).

ID	SHA-256	Storage key	Lock	Retain until
EVD-025	`b30d1be49e21d08ed66d2ea223b5a3d5d5e19d927e08f9d32e2a8313b0126b53`	`s3://wf-ir-evidence/organization-trail/EVD-025.tar.zst`	compliance, hold	July 13, 2033
EVD-026	`981338806a3f2c998cbdfb8ebaba4da7466f1d73349db051db166a7e8c36d945`	`s3://wf-ir-evidence/estate/EVD-026.tar.zst`	compliance, hold	July 14, 2033
EVD-027	`d6ba14fb55e56e5f2dc2456eed4380085b8139b608c6412bc378c3d5609cd6eb`	`s3://wf-ir-evidence/estate/EVD-027.tar.zst`	compliance, hold	July 16, 2033
EVD-028	`f20f0a476149c796d7a31c1c3adc6ed654d0990ed7d04995cb5993b0e08e2429`	`s3://wf-ir-evidence/case-records/EVD-028.tar.zst`	compliance, hold	July 22, 2033
EVD-029	`0e8897cb1b6a0ee803c0b07f313bf7c15c3e7e39ba4208fe0b0a292d6c2d9dc1`	`s3://wf-ir-evidence/case-records/EVD-029.tar.zst`	compliance, hold	August 7, 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, from Vantalect to the custodian, Imani Castell, and from Vantalect to counsel, Diane Whitcombe. Counsel received a copy of every working set that existed on July 24, at the readout, and a copy of the last set on August 7. Each copy was hashed on receipt and matched the register.

Transfers, part 1 of 12 (EVD-001 to EVD-003).

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-001	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-04; released by the custodian; hash re-verified, matched.
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-002	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-04; released by the custodian; hash re-verified, matched.
EVD-003	July 4, 04:10	Wrenfield, wf-prod-data (owner Rafael Quintero)	Charles Sieg	Collected read-only: object copy and metadata read.

Transfers, part 2 of 12 (EVD-003 to EVD-005).

ID	Time (EDT)	From	To	What and what was checked
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-003	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-04; released by the custodian; hash re-verified, matched.
EVD-004	July 4, 04:13	Wrenfield, wf-prod-lending (owner Lucía Brandt)	Charles Sieg	Collected read-only: object copy and metadata read.
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-004	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-04; released by the custodian; hash re-verified, matched.
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-005	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-02; released by the custodian; hash re-verified, matched.

Transfers, part 3 of 12 (EVD-006 to EVD-008).

ID	Time (EDT)	From	To	What and what was checked
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-006	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-02; released by the custodian; hash re-verified, matched.
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.
EVD-007	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-03; released by the custodian; hash re-verified, matched.
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.

Transfers, part 4 of 12 (EVD-008 to EVD-010).

ID	Time (EDT)	From	To	What and what was checked
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-008	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-03; released by the custodian; hash re-verified, matched.
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-009	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-03; released by the custodian; hash re-verified, matched.
EVD-010	July 4, 04:50	Wrenfield, wf-management (owner Imani Castell)	Charles Sieg	Collected read-only: credential report per account.

Transfers, part 5 of 12 (EVD-010 to EVD-012).

ID	Time (EDT)	From	To	What and what was checked
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.
EVD-010	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-03; released by the custodian; hash re-verified, matched.
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-011	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-03; released by the custodian; hash re-verified, matched.
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.

Transfers, part 6 of 12 (EVD-012 to EVD-015).

ID	Time (EDT)	From	To	What and what was checked
EVD-012	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-05; released by the custodian; hash re-verified, matched.
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-013	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-01; released by the custodian; hash re-verified, matched.
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.
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-014	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-02; released by the custodian; hash re-verified, matched.
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.

Transfers, part 7 of 12 (EVD-015 to EVD-017).

ID	Time (EDT)	From	To	What and what was checked
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-015	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-04; released by the custodian; hash re-verified, matched.
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-016	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-04; released by the custodian; hash re-verified, matched.
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 8 of 12 (EVD-017 to EVD-019).

ID	Time (EDT)	From	To	What and what was checked
EVD-017	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-04; released by the custodian; hash re-verified, matched.
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-018	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-05; released by the custodian; hash re-verified, matched.
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.

Transfers, part 9 of 12 (EVD-019 to EVD-021).

ID	Time (EDT)	From	To	What and what was checked
EVD-019	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-04; released by the custodian; hash re-verified, matched.
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.
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-020	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-04; released by the custodian; hash re-verified, matched.
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-021	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-03; released by the custodian; hash re-verified, matched.

Transfers, part 10 of 12 (EVD-022 to EVD-024).

ID	Time (EDT)	From	To	What and what was checked
EVD-022	July 9, 08:40	Vantalect Interceptor, wf-audit (owner Mireille Danvers)	Charles Sieg	Collected read-only: Interceptor 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-022	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-05; released by the custodian; hash re-verified, matched.
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-023	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-01; released by the custodian; hash re-verified, matched.
EVD-024	July 9, 10:20	Wrenfield incident bridge (sponsor Mireille Danvers)	Charles Sieg	Collected read-only: text export.
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.

Transfers, part 11 of 12 (EVD-024 to EVD-027).

ID	Time (EDT)	From	To	What and what was checked
EVD-024	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-05; released by the custodian; hash re-verified, matched.
EVD-025	July 13, 09:30	Wrenfield, wf-log-archive (owner Mireille Danvers)	Charles Sieg	Collected read-only: bucket sync, hash manifest.
EVD-025	July 13, 11:20	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-025	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-01; released by the custodian; hash re-verified, matched.
EVD-026	July 14, 09:45	Wrenfield, the organization (management account owner Imani Castell)	Charles Sieg	Collected read-only: scripted read-only export.
EVD-026	July 14, 15:10	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-026	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-03; released by the custodian; hash re-verified, matched.
EVD-027	July 16, 10:00	Wrenfield, the organization (management account owner Imani Castell)	Charles Sieg	Collected read-only: scripted read-only export.

Transfers, part 12 of 12 (EVD-027 to EVD-029).

ID	Time (EDT)	From	To	What and what was checked
EVD-027	July 16, 14:30	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-027	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-06; released by the custodian; hash re-verified, matched.
EVD-028	July 22, 15:30	Vantalect Interceptor, wf-audit (owner Mireille Danvers)	Charles Sieg	Collected read-only: Interceptor replay, hash manifest.
EVD-028	July 22, 16:40	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.
EVD-028	July 24, 14:20	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-07; released by the custodian; hash re-verified, matched.
EVD-029	August 7, 11:40	Vantalect Interceptor, wf-audit (owner Mireille Danvers)	Charles Sieg	Collected read-only: Interceptor export, hash manifest.
EVD-029	August 7, 12:10	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-029	August 7, 14:40	Charles Sieg	Diane Whitcombe	Counsel's copy of working set WCS-08; hash re-verified, matched.

Disposition of each item

Every item is retained, under counsel's instruction of August 6, 2026, and none is destroyed. Diane Whitcombe of Tessaly & Brook LLP instructed in writing: "Retain every sealed item, keep the legal hold on every object, and release no hold except on counsel's written instruction." The bank's custodian, Imani Castell, holds the evidence account and the key. Vantalect holds no sealed item and no key.

Retention. Counsel set the retention at activation: a legal hold on every object and a 7-year lock. Each object is locked in compliance mode until 7 years after its sealing, which no one can shorten. The hold, not the date, is what keeps an item once those years pass. The retain-until date is in the register. Counsel decides when, if ever, a hold is released.

The disposition of the register.

Disposition	ItemsItem IDs
Retained, compliance lock and legal hold	29EVD-001 to EVD-029
Sealed items destroyed	0None
Released from hold	0None

The disposition of each item (EVD-001 to EVD-008).

ID	Item	Disposition	Retain until	Note
EVD-001	The attacker's lifecycle rule on the imaging bucket, captured before removal	Retained under counsel's instruction	July 4, 2033	
EVD-002	Ransom note in the imaging archive bucket, with object metadata	Retained under counsel's instruction	July 4, 2033	The contact in the note is withheld from every report and from any copy made after counsel's instruction.
EVD-003	Ransom note in the data lake bucket, with object metadata	Retained under counsel's instruction	July 4, 2033	The contact in the note is withheld from every report and from any copy made after counsel's instruction.
EVD-004	Ransom note in the lending documents bucket, with object metadata	Retained under counsel's instruction	July 4, 2033	The contact in the note is withheld from every report. The object's metadata is the only evidence of its write.
EVD-005	GuardDuty and Security Hub exports	Retained under counsel's instruction	July 4, 2033	
EVD-006	The service control policy and resource control policy as attached	Retained under counsel's instruction	July 4, 2033	
EVD-007	Attacker key metadata and policy, prod-lending	Retained under counsel's instruction	July 4, 2033	The key itself stays in the bank's account in the state the bank left it, for counsel; its imported key material expired on July 7 at 18:00, which put it in the PendingImport state. The bank's call to disable it at 10:03:30 on July 8 was rejected with `KMSInvalidStateException` (`EV-01052`), so the key was never disabled; the rejected call is in the trail. It is not an evidence item and is not deleted.

ID	Item	Disposition	Retain until	Note
EVD-008	Attacker key metadata and policy, prod-imaging	Retained under counsel's instruction	July 4, 2033	The key itself stays in the bank's account in the state the bank left it, for counsel; its imported key material expired on July 7 at 18:00, which put it in the PendingImport state. The bank's call to disable it at 10:03:55 on July 8 was rejected with `KMSInvalidStateException` (`EV-01054`), so the key was never disabled; the rejected call is in the trail. It is not an evidence item and is not deleted.

The disposition of each item (EVD-009 to EVD-016).

ID	Item	Disposition	Retain until	Note
EVD-009	Attacker key metadata and policy, prod-data	Retained under counsel's instruction	July 4, 2033	The key itself stays in the bank's account in the state the bank left it, for counsel; its imported key material expired on July 7 at 18:00, which put it in the PendingImport state. The bank's call to disable it at 10:04:20 on July 8 was rejected with `KMSInvalidStateException` (`EV-01056`), so the key was never disabled; the rejected call is in the trail. It is not an evidence item and is not deleted.
EVD-010	IAM credential reports	Retained under counsel's instruction	July 4, 2033	
EVD-011	IAM account authorization details	Retained under counsel's instruction	July 4, 2033	
EVD-012	Jenkins controller logs	Retained under counsel's instruction	July 4, 2033	Logs only. No disk or memory image of the controller was ever taken.
EVD-013	Organization trail log files and digest files, June 29 to July 4	Retained under counsel's instruction	July 4, 2033	
EVD-014	AWS Config snapshots and configuration history	Retained under counsel's instruction	July 4, 2033	
EVD-015	Shared database snapshot copy metadata	Retained under counsel's instruction	July 4, 2033	Metadata only. The snapshot's data was never collected and is not held.
EVD-016	EBS snapshot inventory and Recycle Bin restore records	Retained under counsel's instruction	July 4, 2033	

The disposition of each item (EVD-017 to EVD-024).

ID	Item	Disposition	Retain until	Note
EVD-017	S3 Batch Operations job record and manifest	Retained under counsel's instruction	July 4, 2033	
EVD-018	Loan platform application and load-balancer logs	Retained under counsel's instruction	July 5, 2033	
EVD-019	RDS snapshot inventory and Vault Lock record	Retained under counsel's instruction	July 6, 2033	
EVD-020	Restore verification: the 31 job completion reports and the July 7 scheduled inventory	Retained under counsel's instruction	July 7, 2033	
EVD-021	The IAM objects the attacker created, captured before deletion	Retained under counsel's instruction	July 8, 2033	
EVD-022	Interceptor case database export, as of containment	Retained under counsel's instruction	July 9, 2033	The export is retained. Interceptor's live database in the bank's account is the bank's to keep or retire.
EVD-023	Organization trail log files and digest files, July 4 to July 9	Retained under counsel's instruction	July 9, 2033	
EVD-024	Bridge log	Retained under counsel's instruction	July 9, 2033	Retained as sealed. The bridge's participants' own notes are not part of this register.

The disposition of each item (EVD-025 to EVD-029).

ID	Item	Disposition	Retain until	Note
EVD-025	Organization trail history before the incident window, June 1 to June 28	Retained under counsel's instruction	July 13, 2033	
EVD-026	Estate configuration export: organization, identities, trust paths, and keys	Retained under counsel's instruction	July 14, 2033	
EVD-027	Network exposure and log-source configuration export	Retained under counsel's instruction	July 16, 2033	
EVD-028	Interceptor replay output	Retained under counsel's instruction	July 22, 2033	Retained with the sealed trail items it was generated from; the replay can be re-run from them.
EVD-029	Closure sweep results and seven-day watch record	Retained under counsel's instruction	August 7, 2033	Delivered in the four-week engagement only.

Integrity re-verification

The register was re-verified four times, and each time all hashes matched. The first check was at containment, the last at the close. The check is repeatable: anyone with read access to the bucket can recompute any hash and compare it with the register.

Every re-verification, from containment to the close.

Check	Time (EDT)	By	Items	Result
VER-1	July 9, 12:20	Imani Castell (custodian) and Charles Sieg	24	all hashes matched
VER-2	July 17, 14:30	Imani Castell (custodian) and Charles Sieg	27	all hashes matched
VER-3	July 24, 14:20	Charles Sieg, Diane Whitcombe, and Imani Castell (custodian)	28	all hashes matched
VER-4	August 7, 15:30	Imani Castell (custodian) and Charles Sieg	29	all hashes matched

The method differed by check. VER-1 and VER-2 recomputed each hash from the stored object. VER-3 hashed counsel's copy on receipt and compared it with the register and the stored object. VER-4 recomputed every stored object's hash, read back every Object Lock mode, retention, and legal hold, and recomputed the hash of each of Vantalect's working-copy sets before destruction. The organization trail digest chain was validated over the union of the three sealed trail copies (EVD-013, EVD-023, EVD-025), so the chain is checked across each cut, and no file was reported invalid. The copies are split by delivery time (S3 key and LastModified), not by event time. A file delivered after a cut that holds earlier events is a late file; late files, if any, are listed in the verification output, and the method, not a count, is the point.

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

Vantalect's working copies

Vantalect made 8 working-copy sets from the sealed items. They were never the evidence, and none exists now. Each set groups the working copies of several items. The set hash below is the SHA-256 of the set as it stood when VER-4 recomputed it, before destruction.

The working-copy sets and the items each holds.

Set	Contents	Phase	Items
WCS-01	Organization trail, three windows	Response and investigation	EVD-013, EVD-023, EVD-025
WCS-02	Security services and policies	Response	EVD-005, EVD-006, EVD-014
WCS-03	Identity and keys	Response and investigation	EVD-007, EVD-008, EVD-009, EVD-010, EVD-011, EVD-021, EVD-026
WCS-04	Data stores and ransom notes	Response	EVD-001, EVD-002, EVD-003, EVD-004, EVD-015, EVD-016, EVD-017, EVD-019, EVD-020
WCS-05	Platform logs and case records	Response	EVD-012, EVD-018, EVD-022, EVD-024
WCS-06	Network and log-source configuration	Investigation	EVD-027
WCS-07	Interceptor replay output	Investigation	EVD-028
WCS-08	Closure sweep and watch record	Recovery	EVD-029

Counsel holds a copy of each set, handed over on July 24 (sets `WCS-01` to `WCS-07`) and August 7 (`WCS-08`). Counsel's copies are not covered by the certificate below and are not Vantalect's to destroy. 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.

Certificate of destruction

On August 7, 2026, Vantalect destroyed every working-copy set it held, on counsel's written instruction, and the signer attests to that below. This certificate is a statement of fact about what Vantalect did. Whether it satisfies any duty the bank or counsel has is for counsel to decide.

Counsel's instruction

Diane Whitcombe of Tessaly & Brook LLP instructed Vantalect in writing on August 6, 2026: "Destroy Vantalect's working copies of the sealed items after the final verification (VER-4). Counsel holds a copy of every set. Retain the sealed items and every legal hold." Vantalect set no deletion date of its own, and every sealed item remains in `wf-ir-evidence`.

How the sets were destroyed

- Each working-copy set lived on an encrypted working volume made for this engagement, with its own key, in Vantalect's incident workspace.
- Before destruction, each set's SHA-256 was recomputed and recorded in this log (VER-4, at 15:30).
- Each volume was erased by deleting the volume and the key that encrypted it. Cloud-storage copies of the sets were deleted. A final listing of the working area showed no objects.

The sets destroyed

The working-copy sets destroyed on August 7, by set ID and hash.

Set	Items	SHA-256 of the set before destruction	Destroyed (EDT)
WCS-01	3	3e09fc78d8cf89cc69cf9b4d10cde52f3e670dde883d853de9a60665d05467a5a	August 7, 16:10
WCS-02	3	36bfad92f29b61ba59d6f3e1f9f759528ac16a1ec94dc5c5528de559c1fff3cca	August 7, 16:13
WCS-03	3	75b877522ac9012e4c838b30c6d6fb2be1eb556f1b7132a1373c619715d7b4aa0	August 7, 16:16
WCS-04	3	9114844c10c211150e1510a330cb09f4131a08305fdb62a7074c28a719de3e32b	August 7, 16:19
WCS-05	3	45cdc017e2836d46147e94f0b91b8730b838fbb5e8af7f9fadbdb0ce2b5a59487	August 7, 16:21
WCS-06	3	17d05d80adae56c0c4e9b7ed4e9f5dd4b01a6acbfe6af04cac43f469d1585e436	August 7, 16:23
WCS-07	3	1cdca9635cc1bcfa996410f18c160a27356edd436e3a12444111e304ebe4d01fc	August 7, 16:24
WCS-08	3	11bc9ccfbd46426883180f398497890c12ef078dc45a4a252558e6225582a8e8a	August 7, 16:25

Attestation

1. I am Charles Sieg of Vantalect, LLC. I made and held the working copies listed in this section, and I did the work this certificate describes.
2. I destroyed the sets because counsel instructed Vantalect in writing to do so on August 6, 2026. Vantalect set no deletion date of its own for these copies.
3. The listed sets are all of the working copies Vantalect made from the sealed evidence items. Each was destroyed on the date and at the time shown.
4. To my knowledge, Vantalect now holds no copy of any sealed evidence item. Vantalect's reports quote identifiers, times, and counts from the items, and its engagement records are not evidence copies; this certificate does not cover them.
5. This certificate does not cover the sealed items in `wf-ir-evidence`, which remain under counsel's instruction of August 6, 2026; Interceptor's live data in the bank's account `wf-audit`; or any copy counsel holds.
6. I make no statement about any copy that I did not make or do not hold.

```text
Signed:   Charles Sieg
For:      Vantalect, LLC
Date:     August 7, 2026
Time:     16:25 EDT (destruction completed)
```

The name above is typed. No signature image is attached to this sample.

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.