Vantalect



AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

Executive Brief

DISTRIBUTION: COUNSEL ONLY

Week 2 of 4: Readout · prepared for Wrenfield Bancorp, Inc.

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

July 24, 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

The answer 2
The attack in one figure 3
What it cost 4
Is the attacker out 5
The root causes 6
Decisions and their owners 7
What the Recovery would close 9

Who reads this, and what it does not cover

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. **Distribution:** counsel alone. The brief goes to Diane Whitcombe, who decides who else receives it, forwards it, and keeps the distribution record. It is as of Friday, July 24, 2026 and makes no legal determination: whether any law or rule applies is for the bank and counsel. It holds no witness-interview content, which counsel conveys orally.

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.

The answer

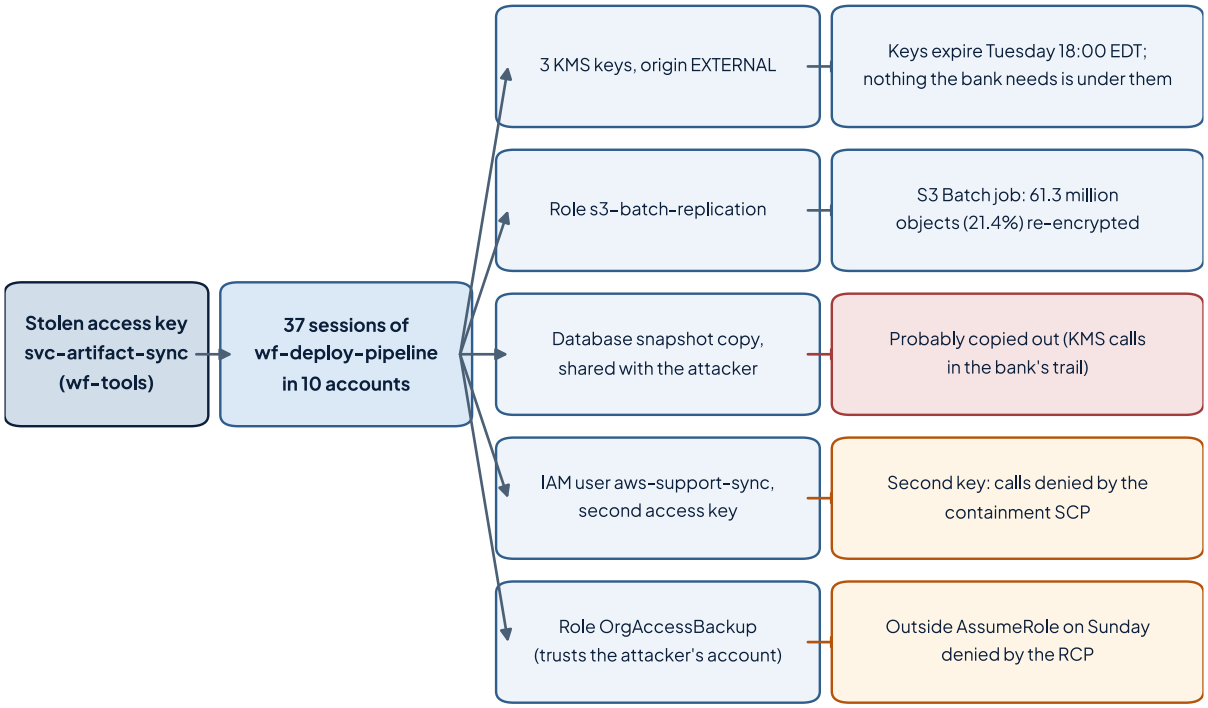
Five sentences say what the Investigation found.

1. **How they got in.** A service user's access key, `svc-artifact-sync`, created March 14, 2023 and never changed, was first used on Monday, June 29 at 03:14 EDT from an address outside the bank, and on the night of Friday, July 3 it let the attacker act as an administrator in ten workload accounts. The AWS logs do not show how the key left the bank.

2. **What they touched.** They created 3 encryption keys of their own, re-encrypted 61.3 million of the imaging archive's 286 million objects, deleted 46 disk and 9 database snapshots (all restored), and shared a copy of the loan database with an account of their own for 137 minutes. The copy-out is probable, with high confidence; the copy holds 412,317 applicants' records.
3. **Whether they are out.** No successful attacker access is recorded since 03:01 EDT on July 4; every later attempt was refused.
4. **What happens next.** The fixes are in the Control Gaps and Fix Plan appendix of the Root Cause report (Report 5), planned for week three of the Recovery. Six decisions below are the bank's.
5. **What is still unknown.** Whether anyone read files in the imaging archive (reads were not logged), and what the attacker has done with the copied records. Our AWS watch cannot see publication or sale; a leak-site monitoring service that the bank or its insurer's vendor retains could, which is outside Vantalect's scope.

The attack in one figure

One long-lived access key led to administrator access in ten accounts, to the attacker's own encryption keys, and to a database copy shared outside the bank, which probably left it. The two lower paths ended in denials: the policies the bank attached on July 4 refused them.



The attacker's credential chain: from the service user's key to what they made, and where each path ended.

What it cost

The attack probably took data (high confidence), took the loan platform offline, and came with a demand for $14,500,000. The bank paid nothing.

What the attack took, what it stopped, and what was demanded. Probable and unknown are stated as such.

Measure	Value
Records in the snapshot shared with the attacker	412,317 loan applicants (names, Social Security numbers, dates of birth, income): New York 389,904, Pennsylvania 15,077, other states 7,336. The bank ran the query on its loan system; Vantalect does not attest to the counts
Whether the records left the bank	Probable, with high confidence. The share was open 137 minutes, to 02:08:20 EDT on July 4. In that time the attacker's account made 7 calls on the lending key (00:06 EDT to 00:51 EDT), including a `ReEncrypt` to a key in its own account
Imaging archive	61.3 million of 286 million objects (21.4%) re-encrypted; the bank rewrote all of them under its own key by Tuesday, July 7, 12:40 EDT. Whether any object was read is unknown, because reads were not logged. No host access was found
Loan origination	Offline 110 hours 10 minutes; 1,912 applications queued, all processed by Friday, July 10
Response hours and the demand	56 hours. The demand was $14,500,000 in cryptocurrency by Tuesday, July 7, 18:00 EDT; nothing was paid

Is the attacker out

No successful attacker access is recorded since 03:01 EDT on Saturday, July 4. That is as far as the bank's logs can show. The organization trail kept recording through the attack, and the attacker's attempt to stop it failed (`EV-00502`).

What was cut, and when, on July 4. The key the attacker came in with was deactivated at 01:24 and its sessions revoked at 01:26. The database snapshot share to the attacker's account (`CI-026`) was removed at 02:08:20 EDT, the outside statement was dropped from the three attacker key policies at 02:09, and the attacker's key grant was revoked at 02:10:30 EDT (`EV-00632` to `EV-00636`); we recorded the settings first. The access key the attacker had created was deactivated at 03:01.

Open on July 24. Two items are planned for week three: deletion protection on `wf-los-prod` (`CI-028`), still off, with the containment policy as the compensating control until it is turned back on July 28; and the legacy account trail the attacker deleted (`CI-019`), which cannot be restored and which the organization trail replaces.

Four tests of whether the attacker is out, with the evidence for each.

Test	Result
After the containment policy	15 attacker calls after 01:22 EDT; 5 denied, 10 sign-ins and reads. None changed or removed data (`EV-00538` to `EV-00644`). At 01:36 EDT the attacker assumed the backup role as an administrator (`EV-00569`); the policy denied its 01:39 EDT attempt to delete the loan database (`EV-00570`)
The second access key	Stayed active until deactivated at 03:01 EDT. Last successful call 02:50 EDT (`EV-00641`), when Pursuit alerted. A policy update at 02:58 EDT (`EV-00642`) denied the attacker's principals; the first denial was at 02:59:30 EDT (`EV-00643`)
The attacker's encryption keys, user, and roles	Key material expired Tuesday, July 7, 18:00 EDT; at 14:00 EDT on Tuesday, July 7 the bank's 31 rewrite completion reports showed 61,300,000 tasks succeeded and 0 failed, and its queries of the archive bucket's live inventory table (Athena, 4 queries) found 0 current business-data object versions under any attacker key (the preserved ransom-note versions are excluded). A scheduled S3 Inventory report cannot be run on demand, so it corroborates that check later and is not its basis. The three keys have been in PendingImport since that expiry; the bank's `DisableKey` calls on Wednesday, July 8 were rejected with `KMSInvalidStateException` (3 of 3), and the keys are kept as they are for counsel. User, access key, and two roles deleted Wednesday, July 8 after preservation (`RE-174` to `RE-180`)

What this does not show. We see the organization trail and the logs we were given; a system that logs nothing, such as reads from the imaging archive, shows us nothing. We assume that a denied call from another account on the bank's key reaches the bank's trail, as the Sunday call does.

The root causes

There are six root causes. Report 5 sets them out, and its Control Gaps and Fix Plan appendix holds the fixes. This brief ranks none of them.

The six root causes and the interim position standing on July 24.

Root cause, in plain terms	In place on July 24
RC-1: A service user's key, unchanged for over three years, was used from outside the bank.	Key deactivated July 4, deleted July 8; build moved by hand
RC-2: A powerful role in every workload account accepted anyone from the tools account.	Trust narrowed by hand on July 8 in all ten accounts
RC-3: No organization rule refused the attacker's own keys, a snapshot shared outside the bank, or a job that rewrites the archive.	Containment policy July 4, 01:22; path out closed 02:08 to 02:10; outside-account policy 03:20 (not yet tested in staging)
RC-4: The imaging archive kept old versions of its files but did not lock them against deletion or expiry.	Not closed on July 24; the attacker's expiry rule removed July 4. Planned: closed for new object versions July 30 (DEC-2, F-5); open for existing objects, planned (F-11, Chief Information Officer, September 30)
RC-5: Nothing alerted on the attacker's first days, and the holiday page took 34 minutes.	Pursuit follows the attacker's principals since July 4; no estate-wide alerts
RC-6: Month-end database snapshots sat in the same account the attacker controlled.	Copies in the vault account since July 5 and 6 (DEC-3)

Decisions and their owners

Six decisions are the bank's, and none waits on us. Each gives who decides, by when, and what follows from each option.

- **DEC-1, Mireille Danvers, Monday, July 27: Whether the week-three fix work goes ahead.** The Control Gaps and Fix Plan appendix of Report 5 lists the fixes and defines critical. Approve: work starts July 27, the items the appendix calls critical are done by July 31, and the production rules follow a test step. Approve in part or later: each item that waits stays open, the bank accepts that in writing, and the August 7 gate does not close for it. Decline: the July 4 interim controls stay the only protection, and the gate cannot be met.

- **DEC-2, Rafael Quintero, Tuesday, July 28: Whether new imaging-archive versions are locked for 30 days.** Object Lock prevents deletion of the protected versions during retention, subject to the governance-mode bypass. It does not prevent a new current version from being written under the same object key, so write and key guardrails are still needed to stop a re-encryption. Retained readable versions support recovery. The lock does not reach the files already there, a residual risk until the bank acts or accepts it in writing. Lock, liftable by bank staff: new versions are protected for 30 days, and a captured administrator could still try to lift it. Lock that nobody can lift: stronger, but nobody can shorten it, including the bank, if it is set in error. No lock: deletion of versions stays possible as on July 3, and the bank accepts that in writing.
- **DEC-3, Mireille Danvers, Friday, July 31: Whether to accept RC-6 in writing, including the limit on the vault-account snapshot copies.** RC-6 is accepted as follows. The central copies in wf-backup remain under governance-mode AWS Backup Vault Lock until the planned compliance-mode cutover next quarter. The ten plain RDS snapshot copies in wf-recovery-vault remain outside Vault Lock and rely on a policy on the vault account and keys the bank holds; a person with Organizations rights in the management account could change that policy. That separate limitation is not cured by the central-vault cutover. Accept until the move: the weak point stays until next quarter. Do not accept: the bank must find another control before the August 7 gate.
- **DEC-4, Diane Whitcombe, standing: How long to keep the attacker's encryption keys and the isolated snapshot copy.** The three attacker encryption keys, their aliases, and the isolated snapshot copy are kept as they are. The outside statement was dropped from each key policy on July 4 at 02:09. The keys have been in PendingImport since their imported key material expired on July 7 at 18:00; the bank's three DisableKey calls of July 8 (10:03 to 10:04) were rejected with KMSInvalidStateException, as AWS does for a key in that state, and the rejections are in the trail. Keep them: the evidence stays complete until counsel releases it. Release earlier: counsel must be sure no claim or request needs them, because they cannot be rebuilt.
- **DEC-5, Diane Whitcombe, after counsel's review: Whether, when, and to whom the indicators of compromise are released.** The indicators let others look for the same attacker. Release: others can search, and the attacker learns which indicators are known. Hold: nothing is shared, and others cannot search.
- **DEC-6, Mireille Danvers, Wednesday, September 30: How contractors reach the bank's cloud accounts.** The question is whether outside people keep any access to the bank's cloud accounts, and on what terms. Identity Center on a bank-managed device: the bank controls the device and the sign-in, and contractors accept its device rules. No contractor access: the bank does the work itself or finds another way.

What the Recovery would close

The Recovery, signed Friday, July 10, is under way. Week 3, July 27 to July 31: The work in the Control Gaps and Fix Plan appendix of Report 5, with the guardrails tested first. On July 28, deletion protection on the loan database goes back on. Week 4, August 3 to August 7: The closure sweep reruns the week-one map and indicator searches and compares them. The seven-day watch, July 31 to August 7, is read. The gate is met when the sweep shows RC-1 to RC-3 closed as code, RC-4 closed for new object versions and open for existing objects (planned, with an owner and a date in the Eradication report), RC-5 closed, RC-6 accepted in writing, no new indicator hit, and a quiet watch. Planned: Friday, August 7.

© 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.