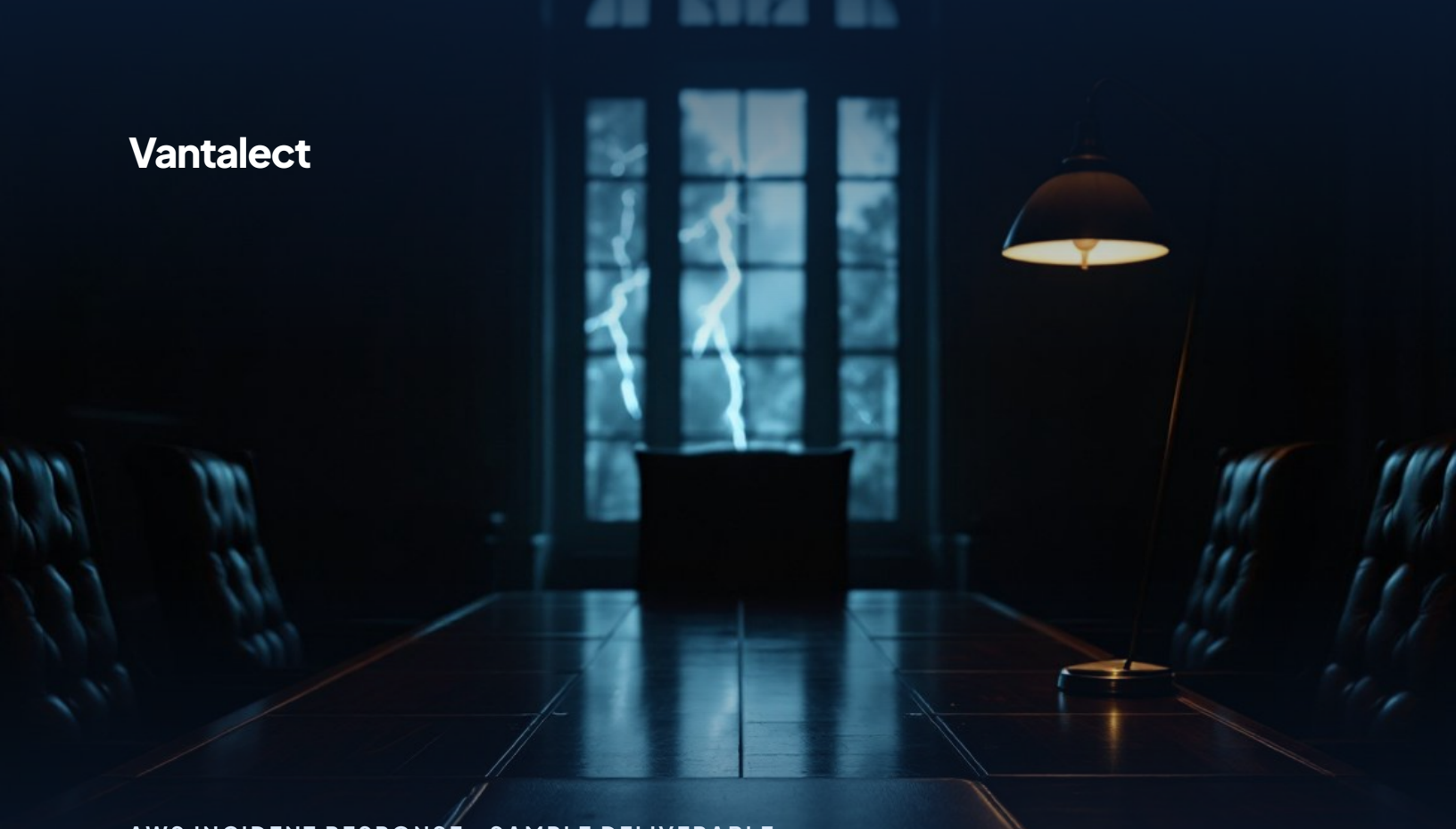


Vantalect

AWS INCIDENT RESPONSE · SAMPLE DELIVERABLE

Executive Brief at Containment

DISTRIBUTION: COUNSEL ONLY

Day 6: Containment declared · 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.

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. Counsel decides whether the Chief Executive and the board receive this brief, forwards it, and keeps the distribution record.

The incident in brief

An attacker used a long-lived access key, used from outside the bank, to enter Wrenfield's cloud accounts, worked read-only from Monday, June 29, and on the night of Friday, July 3 opened its first write-capable session, then deleted backups and locked the loan-document archive under keys only the attacker held, demanding $14,500,000 in cryptocurrency by Tuesday, July 7, 18:00 EDT. We were engaged at 00:52 EDT on Saturday, July 4, the first guardrail went on 4 hours 18 minutes after the attacker's first write-capable session, and by 03:20 that morning every route the attacker held had been closed or blocked: the key it came in with was deactivated at 01:24, its sessions were revoked at 01:26, the loan-database snapshot share was removed at 02:08, the access key it had created was deactivated at 03:01, and a policy against outside accounts was attached at 03:20.

The attacker did get back in once after the first guardrail: at 01:36 it assumed a backup role in the lending account as an administrator, the guardrail stopped only its 01:39 attempt to delete the loan database, and its last successful call was at 02:50.

The bank rewrote every locked object under its own keys before the attacker's keys expired, no payment was made, and loan origination was back online after 110 hours 10 minutes. One loan-database snapshot was shared with the attacker's account for 137 minutes and was probably copied out of the bank, with high confidence, and it holds 412,317 applicants' records; we cannot confirm the copy, and we cannot know whether the attacker read any file in the imaging archive, because those reads were not logged.

What is safe now

- **The attacker's known access is gone.** Both access keys are deactivated, the user and the two roles are deleted, and the build role trusts only the bank's build server.

- **The locked data is readable under the bank's keys.** The bank reports that no archive object is current under an attacker key. It checked on July 7 from the completion reports of its rewrite jobs (no task failed) and a query of the bucket's live inventory table; the query results were not independently preserved. A scheduled S3 Inventory report cannot be run on demand and would later confirm encryption-type coverage, not which KMS key encrypted each version. The attacker's keys have expired and are in PendingImport; the bank's attempts on July 8 to disable them were rejected for that reason, and the keys are kept as they are for counsel.
- **The path out of the bank is closed.** The database snapshot is no longer shared with the attacker's account, the outside statement is gone from the attacker's three key policies, and the attacker's key grant is revoked. All of it was done by 02:11 on July 4.
- **The deleted backups are back, and protected copies exist** in a separate vault account that only two copy roles can enter (the bank's setup role was shut out on Wednesday afternoon), each with MFA and two-person approval. The 46 disk-snapshot copies are under a 14-day compliance lock. The ten database-snapshot copies are not locked: a policy on the vault account and keys the bank holds protect them, and the weak point is anyone with Organizations rights in the management account, who could change that policy.
- **Evidence is preserved** in a separate account, behind a lock that cannot be shortened.
- **Loan origination is back online** after the bank's integrity checks.

What was touched

- **Access:** 37 sessions of the build role in 10 accounts, and 4 identities made (one user, one key, two roles).
- **Keys and data:** 3 encryption keys that only the attacker held, and 61.3 million of the archive's 286 million objects (21.4%) re-encrypted.
- **Backups:** 46 volume snapshots and 9 month-end database snapshots deleted, and all restored.
- **Shared outside the bank (copy-out probable, high confidence):** 1 database snapshot, holding 412,317 applicants' records. It was shared with the attacker's account at 23:51 EDT on July 3. The attacker's account then made 7 calls on the snapshot's key from 00:06 EDT to 00:51 EDT, including a re-encrypt call with a key in its own account as the destination. After we recorded the share's settings, the bank removed it at 02:08:20 EDT.

What is still unknown, and when we will know

- **Whether data left the bank.** Probable, with high confidence; not confirmable. Answer: the readout, Friday, July 24.
- **What was read in the imaging archive.** Not knowable; reads were not logged. Answer: not from the logs.

- **Whether any other foothold remains.** None known; only a sweep can say. Answer: the closure sweep, by August 7.
- **How the key left the bank.** The AWS logs do not show it; counsel holds that question. Answer: the readout, Friday, July 24.
- **Every root cause.** Interim controls are in place on three of the six; none is closed yet, and the rest are not yet assessed. Answer: the readout, Friday, July 24.
- **Whether the attacker will publish or sell the records.** Our AWS watch cannot see publication or sale. Only a service that watches leak sites and markets can: a dark-web or leak-site monitoring service that the bank or its insurer's vendor retains, law-enforcement contacts through counsel, or a credit-monitoring vendor. All three are outside Vantalect's scope. Answer: not from our watch, and outside our scope.

The decisions that are the bank's

We make no legal determination, and we do not say that any rule applies.

- **Notification** (bank and counsel): who else is told, beyond the three notices given.
- **Law enforcement** (General Counsel): how far to cooperate beyond the FBI report.
- **Insurer** (General Counsel, with the broker): the claim and the insurer's view.
- **Communications** (Chief Executive, with counsel): what staff, customers, and the press are told.
- **Monitoring for publication** (General Counsel, with the insurer): whether to retain a leak-site or dark-web monitoring service, since our AWS watch cannot see publication.
- **The demand** (board and counsel): nothing was paid; any further step goes through counsel.
- **Materiality** (bank and counsel): whether and when to determine the incident material.

What we propose next, and what the Response used

We propose the Investigation and the Recovery, Monday, July 13 to Friday, August 7, four weeks, to be signed by Friday, July 10, with the readout on Friday, July 24. The fee is $50,000, less an $8,100 credit for Response hours, $41,900 net. The Response used **56 hours**, $37,800 at $675 an hour, under a not-to-exceed of 80 hours.

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.