

Vantalect

AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

Factual Summary for Regulators, Insurers, and Auditors

DISTRIBUTION: RELEASABLE

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

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.

About this summary

This summary states facts about the Wrenfield Bancorp, Inc. incident as of Friday, August 7, 2026. This report holds facts only, in a form counsel may release. Counsel decides whether, when, and to whom.

It holds facts only, with no analysis, opinion, or legal conclusion. It does not say that any law applies. It holds no cost information, no ransom contact, no credential, and no indicator, and it does not name the party responsible.

What happened

An outside party used an access key issued to a service user to enter the bank's cloud accounts and, on July 3, began destroying and re-encrypting data. The bank attached containment controls at 01:22 EDT on July 4. Times are Eastern Daylight Time, as recorded, and the year is 2026.

The first use of the key found in the logs was June 29, 03:14 EDT, from an address outside the bank's networks. Activity was read-only until the first write-capable session in production began at 21:04 EDT on Friday, July 3. Containment was declared in writing at 09:00 EDT on Thursday, July 9.

The alert, the page, and the confirmation of the note, each with who recorded it.

Date and time (EDT)	Event	Recorded by
Friday, July 3, 22:44	An automated alert was raised in the bank's audit account and forwarded to the provider.	The alert record and the provider
Friday, July 3, 23:18	The provider paged the bank's on-call cloud engineer.	The provider
Saturday, July 4, 00:05	The on-call engineer confirmed the ransom note and called the Cloud Platform Lead and the Chief Information Security Officer.	The bank

The bank's recorded date of initial detection is Saturday, July 4.

Systems affected

Loan origination was offline for 110 hours 10 minutes, and the bank restored every deleted backup and every re-encrypted object. The configuration of one legacy account trail was deleted and was not recreated. The bank took loan origination offline at 01:50 EDT on July 4 to freeze its state, and it returned at 16:00 EDT on Wednesday, July 8. A total of 1,912 applications queued and were processed by Friday, July 10.

- **Imaging archive.** The archive (286 million objects) holds loan files, check images, and signature cards. At 21:41 EDT on July 3 a session of the build role the key had assumed created an S3 Batch Operations job, which runs under a role created in the same session. For each object it processed, the job copied the object onto itself inside S3 as a new version encrypted under a key the attacker had made. It processed 61,300,000 objects (21.4%), its completion report was off, and the bank canceled it at 01:28 EDT on July 4, after 3 hours 47 minutes. The archive does not log object reads, so the logs neither show nor exclude reads. The bank rewrote the objects under its own key by 12:40 EDT on July 7. At 14:00 EDT that day the bank checked the result from the 31 jobs' completion reports (61,300,000 tasks succeeded, 0 failed) and from 4 queries of the bucket's S3 Metadata live inventory table, begun at 13:50 EDT. The queries showed 0 current business-data object versions under any attacker key (the preserved ransom-note versions are excluded) and 286,000,000 under the bank's key. The earlier versions that remained under the attacker keys (61,300,000) were noncurrent. A scheduled S3 Inventory report is not run on demand and was not the check.
- **Backups.** 46 disk snapshots and 9 database snapshots were deleted, and the bank restored all of them.
- **Attacker-created items.** 3 encryption keys, one user with its access key, two roles, and a ransom note in each of three buckets. The user, key, and roles were deleted on July 8, and the keys were kept as they are. One legacy account trail was deleted, and the organization-wide trail kept recording.
- **No payment.** The note demanded $14,500,000 in cryptocurrency by 18:00 EDT on Tuesday, July 7. No payment was made.

Data and records

The database snapshot named in the sharing event holds 412,317 loan applicants' records: names, Social Security numbers, dates of birth, and income.

Applicant records by state of residence, from a query the bank ran on its loan system.

State of residence	Applicant records
New York	389,904
Pennsylvania	15,077
Other states	7,336
Total	412,317

Source of the counts. The counts come from queries the bank ran on its own systems; Vantalect does not attest to them. The bank's lending operations team (owner Lucía Brandt, Head of Lending Operations) ran the count of applicant records on Sunday, July 5, 08:40 EDT and the split by state of residence on Monday, July 20, 16:40 EDT, and gave each result to counsel. Counsel's file holds them (references `CF-001` and `CF-002` in the Chain-of-Custody Log). Vantalect did not collect the snapshot's data.

These are the logged events about the snapshot, and no more:

- A copy of the snapshot was shared with the outside account `777788889999` at 23:51 EDT on July 3.
- From 00:06:09 EDT to 00:51:06 EDT on July 4, 7 calls on the key that protected the copy were logged in the bank's account: two `CreateGrant` (one naming a role in that outside account as grantee), one `DescribeKey`, one `ReEncrypt` with a destination key in that outside account, two `Decrypt`, and one `RetireGrant`.
- At 02:08:20 EDT on July 4 the bank removed that account from the snapshot, after 137 minutes. At 02:09 EDT it dropped the outside statement from three key policies, and at 02:10:30 EDT it revoked the grant.

No host access to any instance was observed in the control-plane records, and the loan platform's application and load-balancer logs show no known attacker traffic. No host image or host telemetry was collected, so host compromise cannot be ruled out with this evidence.

Containment and recovery

- On July 4 the bank attached the containment policy at 01:22 EDT, deactivated the service user's key at 01:24 EDT, and revoked active sessions at 01:26 EDT. At 01:36 EDT a session from the outside account assumed a backup role in the lending account, and the containment policy denied its 01:39 attempt to delete the loan database. The last successful call by an attacker session was at 02:50 EDT. The bank deactivated the second access key at 03:01 EDT and attached a resource control policy at 03:20 EDT.
- The bank preserved evidence in a separate account, then on Wednesday, July 8 deleted the attacker-created user, its access key, and two roles, and replaced the service credential with a role-based sign-in. The three attacker encryption keys were kept as they are for counsel. Their imported key material expired at 18:00 EDT on July 7, which put each key in the PendingImport state. On July 8, from 10:03:30 to 10:04:20 EDT, the bank's call to disable each key was rejected with `KMSInvalidStateException`, so no key was disabled and no change to the keys succeeded that day. The statement naming the outside account had been dropped from each key policy at 02:09 EDT on July 4.
- In the recovery vault account, the 46 disk snapshot copies are under a 14-day compliance-mode lock. The 10 database snapshot copies are plain snapshots, protected by an organization policy and by keys the bank holds. A replication rule from the imaging archive to a bucket in that account was set on July 8; the rule copies only objects created after it was set. To copy the existing objects the bank built a manifest of the current versions under its own key and started an S3 Batch Replication job over them at 18:25 EDT that day. The job finished at 21:40 EDT on Sunday, July 12, 4 days 3 hours 15 minutes later: 286,000,000 current versions were in the manifest, 1,206 tasks failed (`SrcVersionNotFound`, the version was gone from the source), and the 122,600,000 noncurrent versions were not in the manifest.
- Between July 27 and July 31 the bank changed its credential, role-trust, organization-policy, storage, and logging settings.

Notices and law-enforcement contact, as recorded

Notices and contacts as the bank recorded them.

Date and time (EDT)	Recorded by the bank
July 4, 06:00	Reported to the FBI field office. IC3 complaint filed at 09:40.
July 4, 14:30	FDIC notified.
July 4, 14:45	Federal Reserve notified.
July 5, 11:15	New York Department of Financial Services notified.
July 17	Form 8-K filed.
July 29	Notices mailed to affected individuals.

Current status

As of August 7, the access paths found were closed, and the affected data and systems were restored. One legacy account trail's configuration stays deleted, and the organization trail supplies the coverage. The closure sweep repeated the week-one searches on the trail and the map. A seven-day watch began on July 31, and this summary states no watch result.

Contact

Diane Whitcombe, Partner, Tessaly & Brook LLP (outside counsel to Wrenfield Bancorp, Inc.). Please direct every question about this summary to counsel.

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.