



As we are moving forward in the new year and now that our forensic investigation has concluded, we wanted to provide an update about our response to the security incident.

Forensic Investigation

The incident was contained, the threat actor was eradicated from the Evolve environment, and the forensic investigation for data owners is now closed. There is no evidence of ongoing persistence of the threat actor in the network, and all known vectors for access by the threat actor and unauthorized software have been removed. As previously stated, this incident did not involve encrypting malware or ransomware.

Data Impact

The Company has determined that the impacted data includes, among other things,

- (i) Evolve corporate files that generally include legal contracts and accounting documents,
- (ii) Files associated with our Corporate Administration activities
- (iii) A smaller number of other records related to various other businesses at Evolve and
- (iv) Records associated with loan file due diligence and underwriting.

There is no evidence that any of its applications or databases (including, but not limited to, CLDD UAT, UW UAT, Client, Brooks, etc.) or file shares associated with any business, other than those mentioned above, have been impacted.

Data Review Process

Evolve worked with counsel and leading experts on the data review, including searching for any consumer personally identifiable information (PII) or sensitive confidential information that may have been involved in this incident.

The data review is now completed, and Evolve, in conjunction with clients, worked on modifying consumer notices for each client to ensure compliance with applicable regulations and improve clarity for recipients. Because the TA took only backup databases of Evolve's UAT system, no PII was available to



them electronically in those records. The TA did take images belonging to certain loans that may or may not have contained PII. The Evolve team worked tirelessly and expeditiously to complete the data mining review of those images in conjunction with our counsel and clients, for the presence of PII, to determine impacted consumers.

Remediation Steps Post Incident

Evolve has taken the steps necessary to address this event and is committed to fully protecting all of the information that is entrusted to us. Upon learning of this event, Evolve immediately took steps to secure its network and undertook a thorough investigation. Evolve with its cyber security expert partners also implemented additional technical safeguards to further enhance the security of information in its possession and to prevent similar events from happening in the future even though the available evidence suggests it was the F5 vulnerability as root cause.

We have taken the following steps:

- Installed F5 patch upon receipt on 10-15-25
- Implemented centralized Logging Platform to ensure logs are not overwritten.
- Modified logging configurations to leverage new platform.
- Notified law enforcement.
- Notified State and other Regulators.
- Enterprise-wide password reset and strengthened password requirements.
- Accelerated implementation of MFA on Web applications that were scheduled for later dates.
- Implemented new technical safeguards.
- Replaced SFTP vendor out of abundance of caution.
- Strengthened encryption processes for data at rest.
- Upgraded Endpoint Detection & Response (EDR) agents and established 24/7 monitoring.
- Performed External Network Penetration Test (EPT) (Zero Critical or High found)
- Renewal of prior Web Application Penetration Test (APT) (currently in process) Prior renewal scheduled for 10-1-25 was interrupted by the Incident.
- Scheduled Internal Penetration Test (IPT) to begin at completion of Web application testing.
- Installed Intrusion Detection System (IDS/IPS) (UniFi Gateway Intrusion Detection and Prevention)
- Data Loss Prevention System (DLP) at completion of Internal Penetration Test (IPT) estimated- March 2026
- Reviewing/revised policies and procedures relating to data security
- Additional training/retraining of workforce members



- Annual third-party network security assessments

Going Forward

We expect this to be our last update until the consumer notification process is complete. Customers are being contacted and Consumer Notices are being mailed. Evolve offered complimentary credit monitoring and identity protection services to notified individuals at lengths required per state and/or PII taken and provided call center support.

Thank you again for your continued patience and partnership and your trust in Evolve. If you have questions, please reach out to paul.anselmo@evolvemortgageservice.com.