NAM A BANK

NAM A BANK – HỘI SỞ
201-203 Cách Mạng Tháng Tám, P.Bàn Cờ, TP.HCM
[T] 028 3929 6699 - [F] 028 3929 6688
[Hotline] 1900 6679 - [W] www.namabank.com.vn

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 2526../2026/TB-NHNA-P.26

Tp.Hồ Chí Minh, ngày 20 tháng 08 năm 2026

THÔNG BÁO MỜI CHÀO GIÁ

Chào giá cạnh tranh đánh giá an toàn bảo mật hệ thống giao dịch trực tuyến

Kính gửi: QUÝ CÔNG TY

Ngân hàng TMCP Nam Á (Nam A Bank) có nhu cầu triển khai đánh giá an toàn bảo mật hệ thống giao dịch trực tuyến, hình thức lựa chọn đối tác theo phương thức chào giá cạnh tranh.

Nay Nam A Bank kính mời các Công ty có đủ năng lực, kinh nghiệm và điều kiện tham gia chào giá cạnh tranh theo các nội dung hướng dẫn cụ thể như sau:

I. Mô tả yêu cầu:

1. Nội dung công việc:

- Tấn công thử nghiệm (pentest) hệ thống giao dịch trực tuyến của Nam A Bank (tên thương mại là Nam A Bank Open Banking), bao gồm nền tảng web (https://ops.namabank.com.vn) và mobile (Android và iOS).
- Chi tiết yêu cầu về pentest: Phụ lục 01 chi tiết đính kèm.

2. Tiêu chuẩn về đối tác:

- Có giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng còn hiệu lực.
- Có kinh nghiệm trên 3 năm trong lĩnh vực tấn công thử nghiệm.
- Đã từng thực hiện các dự án tương tự cho các ngân hàng trong vòng 1 năm tính từ thời điểm chào giá.

3. Thời gian thực hiện dự kiến:

- Thời gian dự kiến thực hiện từ tháng 09/2026.

4. Các điều kiện khác:

- Nam A Bank được quyền thay đổi các yêu cầu kĩ thuật và điều kiện triển khai theo nhu cầu thực tế để đảm bảo đem lại hiệu quả cao nhất cho hệ thống Internet Banking.

II. Một số yêu cầu về Hồ sơ chào giá (HSCG):

- Hồ sơ chào giá phải được đóng gói trong phong bì dán kín, các giấy tờ trong Hồ sơ phải có chữ ký của Người đại diện theo pháp luật và đóng dấu của Công ty. Hồ sơ chào giá bao gồm 01 bản gốc và 01 bản sao.
- Hồ sơ chào giá bao gồm:
  + Hồ sơ năng lực của Nhà cung cấp: Báo cáo tài chính 01 năm gần nhất, Giấy chứng nhận đăng ký kinh doanh, Giấy phép đăng ký mã số thuế, Tờ khai quyết toán thuế thu nhập doanh nghiệp năm gần nhất.

+ Tài liệu minh chứng về tiêu chuẩn đã nêu tại mục I.2 Tiêu chuẩn về đối tác.
+ Bảng chào giá chi tiết.
+ Đồng tiền trong hồ sơ chào giá: bằng đồng Việt Nam, giá chào phải bao gồm tất cả các khoản thuế, phí cần thiết.
+ Hồ sơ chào giá phải có hiệu lực tối thiểu 90 ngày.

III. Thời gian và địa điểm nhận Hồ sơ chào giá:

- Thời gian gửi Hồ sơ chào giá: trước 14 giờ 00 phút ngày 27/08/2026. Các Hồ sơ gửi sau thời gian nêu trên, Nam A Bank sẽ xem xét chấp nhận hoặc không chấp nhận tùy theo tình hình thực tế và phù hợp với quy định.
- Nơi nhận Hồ sơ: Phòng An Ninh Thông Tin - Nam A Bank tại số 201 – 203 Cách Mạng Tháng Tám, Phường Bàn Cờ, TP. Hồ Chí Minh.

Nam A Bank kính mời Quý Công ty quan tâm nộp Hồ sơ chào giá theo thời gian và địa chỉ nêu trên.

Mọi vướng mắc trong quá trình lập Hồ sơ chào giá, Quý Công ty vui lòng liên hệ Ông Nguyễn Anh Dũng – Phòng An Ninh Thông Tin (Điện thoại: 028 3929 6699 - Ext: 70302).

Trân trọng./.

Nơi nhận:
- Như trên;
- Lưu: P.HCQT, P. QLHT, P.ANTT.

KT. TỔNG GIÁM ĐỐC
PHÓ TỔNG GIÁM ĐỐC

M.S.D.N: 0300872315 - C.T.C.P
NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN NAM Á
THÀNH PHỐ HỒ CHÍ MINH

Nguyễn Vĩnh Tuyên

PHỤ LỤC 01

Yêu cầu chi tiết đánh giá an toàn bảo mật hệ thống giao dịch trực tuyến

(Ban hành kèm theo Thông báo số 2528/2026/TB-NHNA-P.26 ngày 20/08/2026 của Tổng Giám đốc Ngân hàng TMCP Nam Á)

1. Mô tả chung

Nam A Bank có nhu cầu đánh giá độc lập mức độ an toàn của các kênh Open Banking cung cấp dịch vụ trực tuyến cho khách hàng. Phạm vi dự kiến bao gồm website Open Banking, ứng dụng Mobile Banking trên iOS và Android, API công khai/đối tác và các luồng nghiệp vụ, xác thực, giao dịch, dữ liệu có liên quan.

2. Mục tiêu

- Phát hiện và xác minh các điểm yếu có thể bị khai thác trong điều kiện thực tế.
- Đánh giá rủi ro đối với tài khoản khách hàng, dữ liệu, giao dịch tài chính và hoạt động ngân hàng.
- Đánh giá chuyên sâu logic nghiệp vụ, API, ứng dụng di động và khả năng tác động vào tài khoản.
- Cung cấp khuyến nghị xử lý cụ thể, có thể kiểm chứng.
- Thực hiện retest và xác nhận trạng thái khắc phục.
- Đánh giá mức độ tuân thủ của Open Banking so với các yêu cầu tuân thủ của Thông tư 50/2024/TT-NHNN quy định về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng và Thông tư số 77/2025/TT-NHNN sửa đổi, bổ sung một số điều của Thông tư số 50/2024/TT-NHNN.
- Cung cấp báo cáo quản trị phù hợp Ban TGĐ/HĐQT và báo cáo kỹ thuật phục vụ các đơn vị triển khai.

3. Kết quả mong đợi

- Danh mục phát hiện được phân loại và ưu tiên rõ ràng.
- Bằng chứng kỹ thuật đủ để tái hiện nhưng được kiểm soát để không làm lộ dữ liệu nhạy cảm không cần thiết.
- Phân tích chuỗi tấn công và tác động nghiệp vụ đối với các phát hiện trọng yếu.
- Kế hoạch khắc phục ưu tiên và báo cáo đóng phát hiện sau retest.
- Báo cáo đánh giá mức độ tuân thủ của Open Banking so với các yêu cầu tuân thủ của Thông tư 50/2024/TT-NHNN quy định về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng và Thông tư số 77/2025/TT-NHNN sửa đổi, bổ sung một số điều của Thông tư số 50/2024/TT-NHNN.

4. Phạm vi dịch vụ

4.1. Phạm vi chức năng

Hạng mục	Phạm vi tối thiểu
Open Banking/Web	Đăng nhập, đăng ký, quên/đổi mật khẩu, MFA/OTP, quản lý phiên, hồ sơ khách hàng, người thụ hưởng, chuyển tiền, thanh toán, tra soát, thông báo và các chức năng tài chính liên quan.
Mobile Banking iOS	Phân tích tĩnh/động, lưu trữ cục bộ, giao tiếp, xác thực, quản lý phiên/token, root/jailbreak, hook, giả lập, certificate pinning, chống dịch ngược và các luồng nghiệp vụ.
Mobile Banking Android	Phân tích tĩnh/động, lưu trữ cục bộ, giao tiếp, xác thực, quản lý phiên/token, root, hook, giả lập, certificate pinning, chống dịch ngược và các luồng nghiệp vụ.
API Open Banking	API xác thực, khách hàng, tài khoản, giao dịch, thanh toán, chuyển tiền, người thụ hưởng, thông báo và API public/external/partner khác trong phạm vi.
Logic nghiệp vụ	Luồng xác thực, đăng ký/kích hoạt, người thụ hưởng, hạn mức, chuyển tiền, thanh toán, tra soát, trạng thái giao dịch, xử lý đồng thời và chống gian lận.
Hạ tầng tiếp xúc Internet liên quan	Tên miền, cổng/dịch vụ, TLS, cấu hình bảo mật lớp giao tiếp, API gateway/WAF ở mức được phê duyệt; không bao gồm kiểm thử gây gián đoạn.
eKYC	Chống giả mạo, replay, liveness, thao túng luồng, thay thế dữ liệu/hình ảnh và bypass kiểm soát nghiệp vụ.

4.2. Thông tin phạm vi chi tiết

Danh sách URL, tên miền, IP, API endpoint, phiên bản ứng dụng, môi trường, tài khoản và luồng nghiệp vụ sẽ được Nam A Bank xác nhận với nhà cung cấp được lựa chọn trước khi thực hiện. Nhà cung cấp phải đưa ra đơn giá/cơ chế điều chỉnh minh bạch khi phạm vi thực tế thay đổi.

4.3. Nội dung không thực hiện hoặc ngoài phạm vi

- Tấn công từ chối dịch vụ hoặc tạo tải gây ảnh hưởng môi trường.
- Tác động vật lý vào hệ thống.
- Thay đổi, xóa hoặc làm sai lệch dữ liệu thật.
- Khai thác sang hệ thống không thuộc danh sách được phê duyệt.
- Đánh giá mã nguồn.

5. Yêu cầu kỹ thuật và phương pháp

5.1. Chuẩn và tài liệu tham chiếu

Các chuẩn và tài liệu có thể dùng tham chiếu trong quá trình đánh giá và báo cáo gồm:

- OWASP Web Security Testing Guide (WSTG).

- OWASP Mobile Application Security Testing Guide (MASTG/MSTG) và Mobile Application Security Verification Standard (MASVS), phiên bản phù hợp tại thời điểm thực hiện.
- OWASP API Security Top 10, phiên bản phù hợp tại thời điểm thực hiện.
- Penetration Testing Execution Standard (PTES).
- NIST SP 800-115.
- PCI DSS v4.0.1 đối với các yêu cầu kiểm thử bảo mật có liên quan, nếu áp dụng cho phạm vi.
- CVSS phiên bản phù hợp tại thời điểm báo cáo, kết hợp điều chỉnh theo tác động nghiệp vụ thực tế.
- Các tài liệu khác theo phương pháp luận của đối tác.

5.2. Cách tiếp cận kiểm thử

- Kết hợp black-box và grey-box; sử dụng tài khoản có nhiều vai trò/quyền để đánh giá phân tách truy cập.
- Ưu tiên kiểm thử thủ công đối với xác thực, phân quyền, giao dịch, logic nghiệp vụ và chuỗi tấn công.
- Công cụ tự động chỉ dùng để hỗ trợ phát hiện và xác minh; mọi phát hiện phải được kiểm chứng để loại bỏ false positive.
- Kiểm thử phải thể hiện được điều kiện, bước tái hiện, bằng chứng, tài sản ảnh hưởng, tác động kỹ thuật, tác động đối với ngân hàng và khuyến nghị.

5.3. Lưu ý khi kiểm tra tài khoản và khả năng gian lận giao dịch

- Cần xây dựng chuỗi chiếm/lợi dụng tài khoản phù hợp: credential attack, khôi phục tài khoản, token/session theft, device trust bypass và thay đổi thông tin bảo mật.
- Mô phỏng chiếm quyền nhưng không thực hiện giao dịch gây tổn thất; sử dụng dữ liệu/tài khoản kiểm thử được cấp.
- Đánh giá khả năng chuyển tiền trái phép, đổi người thụ hưởng, sửa giá trị giao dịch, replay và tạo giao dịch hàng loạt trong điều kiện kiểm soát.
- Với từng kịch bản phải nêu rõ điều kiện, khả năng khai thác, kiểm soát đã vượt qua, dữ liệu/giao dịch ảnh hưởng và dấu hiệu giám sát có thể phát hiện.

6. Quy tắc triển khai và kiểm soát an toàn

- Chỉ thực hiện trên tài sản, môi trường, khung thời gian và nguồn IP đã được Nam A Bank phê duyệt bằng văn bản hoặc qua email.
- Có kế hoạch kiểm thử, Rules of Engagement, danh sách nhân sự, đầu mối liên hệ và phương án dừng khẩn cấp trước khi bắt đầu.
- Không thực hiện DoS/DDoS, phá hoại, xóa/sửa dữ liệu thật, tạo tải lớn hoặc hành vi có khả năng làm gián đoạn dịch vụ nếu chưa có phê duyệt riêng.
- Dừng ngay kịch bản liên quan khi phát hiện nguy cơ ảnh hưởng sản xuất và thông báo đầu mối Nam A Bank.

- Khi phát hiện lỗi critical hoặc dấu hiệu bị xâm nhập đang diễn ra phải được thông báo khẩn theo kênh thống nhất, không chờ báo cáo cuối kỳ.
- Dữ liệu thu thập phải tối thiểu hóa, mã hóa khi truyền/lưu, giới hạn truy cập, ghi nhận người sử dụng và xóa theo xác nhận khi kết thúc.
- Không đưa dữ liệu, mã nguồn, thông tin cấu hình hoặc kết quả của Nam A Bank lên dịch vụ AI công cộng, kho chia sẻ công cộng hoặc hệ thống bên thứ ba chưa được phê duyệt.
- Công cụ và thiết bị thực hiện phải được kiểm soát; nhà cung cấp chịu trách nhiệm về bản quyền, an toàn và nguồn gốc công cụ.
- Không thuê thầu phụ nếu chưa được Nam A Bank chấp thuận bằng văn bản; nhà cung cấp chính chịu trách nhiệm toàn bộ.
- Lưu đầy đủ nhật ký hoạt động kiểm thử để phục vụ đối soát khi được yêu cầu.

7. Sản phẩm bàn giao

7.1. Danh mục sản phẩm cần bàn giao

Sản phẩm	Nội dung bắt buộc
Kế hoạch	Phạm vi, phương pháp, lịch, tài khoản, nguồn IP, giới hạn, liên hệ khẩn, tiêu chí dừng.
Báo cáo nhanh về Critical/High (nếu có)	Thông báo sớm, bằng chứng tối thiểu, tác động, biện pháp giảm thiểu khẩn cấp.
Báo cáo quản trị (Executive Report)	Tổng quan, mức rủi ro, phát hiện trọng yếu, tác động khách hàng/ngân hàng, nhóm rủi ro mất tiền/ATO/rò rỉ dữ liệu, ưu tiên xử lý.
Báo cáo kỹ thuật chuyên sâu (Technical Report)	Chi tiết từng phát hiện, CVSS, tài sản, vai trò, bước tái hiện, request/response đã che dữ liệu, PoC, tác động, nguyên nhân, khắc phục, tham chiếu.
Báo cáo chuỗi tấn công	Mối liên hệ giữa các phát hiện và kịch bản gây mất/lạm dụng tài khoản, mất tiền, truy cập dữ liệu hoặc leo thang quyền.
Phiên trình bày kết quả	Ít nhất 01 phiên trình bày kết quả.
Báo cáo Retest	Kết quả từng phát hiện: Closed, Partially Fixed, Open, Risk Accepted/Not Retested; kèm bằng chứng.
Tài liệu đóng dự án	Xác nhận bàn giao, xóa dữ liệu và tổng hợp phạm vi đã thực hiện/chưa thực hiện.

7.2. Yêu cầu trình bày đối với các lỗi được phát hiện

Với mỗi lỗi được phát hiện, yêu cầu trình bày tối thiểu như sau:

- Mã phát hiện và tiêu đề ngắn gọn.

- Tài sản, môi trường, URL/API/chức năng và vai trò bị ảnh hưởng.
- Mức độ nghiêm trọng, điểm/vector CVSS và lý do điều chỉnh theo tác động nghiệp vụ.
- Mô tả, điều kiện tiên quyết, bước tái hiện, bằng chứng và kết quả quan sát.
- Tác động kỹ thuật và tác động đối với ngân hàng: mất tiền, mất/bị lạm dụng tài khoản, rò rỉ dữ liệu, gián đoạn, gian lận hoặc ảnh hưởng tuân thủ nếu có căn cứ.
- Khuyến nghị ngắn hạn và giải pháp xử lý tận gốc.
- Tham chiếu nhóm CWE/OWASP phù hợp và trạng thái retest.