NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 50 /2024/TT-NHNN	*Hà Nội, ngày 31 tháng 10 năm 2024*

THÔNG TƯ
Quy định về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng

Căn cứ Luật Ngân hàng Nhà nước Việt Nam ngày 16 tháng 6 năm 2010;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Luật Các tổ chức tín dụng ngày 18 tháng 01 năm 2024;

Căn cứ Nghị định số 102/2022/NĐ-CP ngày 12 tháng 12 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;

Theo đề nghị của Cục trưởng Cục Công nghệ thông tin;

Thống đốc Ngân hàng Nhà nước Việt Nam ban hành Thông tư quy định về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh

Thông tư này quy định các yêu cầu bảo đảm an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng, bao gồm:

a) Hoạt động ngân hàng và các hoạt động kinh doanh khác của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài;

b) Hoạt động cung ứng dịch vụ trung gian thanh toán;

c) Hoạt động thông tin tín dụng.

2. Đối tượng áp dụng

Thông tư này áp dụng đối với các tổ chức tín dụng, chi nhánh ngân hàng

nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, công ty thông tin tín dụng (sau đây gọi chung là đơn vị).

Điều 2. Giải thích từ ngữ và thuật ngữ

Trong Thông tư này, các từ ngữ dưới đây được hiểu như sau:

1. *Dịch vụ trực tuyến trong ngành Ngân hàng* (gọi tắt là dịch vụ Online Banking) là dịch vụ quy định tại khoản 1 Điều 1 Thông tư này được các đơn vị cung cấp cho khách hàng trên môi trường mạng để thực hiện các giao dịch điện tử (gọi tắt là giao dịch), không bao gồm các giao dịch trực tiếp tại các đơn vị chấp nhận thanh toán qua thiết bị chấp nhận thẻ tại điểm bán, qua Mã phản hồi nhanh (Quick Response Code - QR Code) hiển thị từ phía khách hàng.

2. *Hệ thống Online Banking* là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu, hệ thống mạng truyền thông và an toàn, bảo mật để sản xuất, truyền nhận, thu thập, xử lý, lưu trữ và trao đổi thông tin số phục vụ cho việc quản lý và cung cấp dịch vụ Online Banking, do đơn vị thiết lập, quản trị, vận hành hoặc thuê bên thứ ba thiết lập, quản trị, vận hành.

3. *Phần mềm ứng dụng Online Banking* là phần mềm ứng dụng cung cấp dịch vụ Online Banking.

4. *Phần mềm ứng dụng Mobile Banking* là phần mềm ứng dụng Online Banking được cài đặt trên thiết bị di động.

5. *Giao dịch thanh toán trực tuyến* là giao dịch thanh toán được thực hiện bằng phương tiện điện tử thông qua hệ thống Online Banking.

6. *Khách hàng* là các tổ chức, cá nhân sử dụng dịch vụ Online Banking.

7. *Phương thức xử lý xuyên suốt (Straight-Through Processing)* là phương thức trao đổi thông tin, dữ liệu, tài liệu hai chiều tự động, thông qua kết nối an toàn giữa hệ thống thông tin của khách hàng với hệ thống Online Banking.

8. *Xác nhận giao dịch điện tử (sau đây gọi là xác nhận giao dịch)* là hình thức xác nhận bằng phương tiện điện tử để thể hiện sự chấp thuận của khách hàng đối với các thông điệp dữ liệu trong giao dịch điện tử.

9. *Mã hóa điểm đầu đến điểm cuối (end to end encryption)* là cơ chế mã hóa an toàn thông tin ở điểm đầu trước khi gửi đi và chỉ được giải mã sau khi nhận được tại điểm cuối trong quá trình trao đổi thông tin giữa các ứng dụng, các thiết bị trong hệ thống nhằm hạn chế rủi ro bị lộ, lọt thông tin trên đường truyền.

10. *Hệ quản trị cơ sở dữ liệu* là phần mềm được thiết kế để quản lý, lưu trữ, truy xuất và thực thi các truy vấn dữ liệu trong cơ sở dữ liệu.

Điều 3. Nguyên tắc chung về bảo đảm an toàn, bảo mật hệ thống thông tin cho việc cung cấp dịch vụ Online Banking

1. Hệ thống Online Banking phải tuân thủ quy định về bảo đảm an toàn hệ thống thông tin cấp độ 3 trở lên theo quy định của pháp luật về bảo đảm an toàn

hệ thống thông tin theo cấp độ, đối với hệ thống thông tin cung cấp dịch vụ chuyển mạch tài chính, dịch vụ bù trừ điện tử phải tuân thủ quy định về bảo đảm an toàn hệ thống thông tin cấp độ 4 trở lên; tuân thủ tiêu chuẩn TCVN 11930:2017 (tiêu chuẩn Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ) và quy định của Ngân hàng Nhà nước về an toàn hệ thống thông tin trong hoạt động ngân hàng.

2. Bảo đảm tính bí mật, tính toàn vẹn của thông tin khách hàng; bảo đảm tính sẵn sàng của hệ thống Online Banking để cung cấp dịch vụ một cách liên tục.

3. Các giao dịch của khách hàng được phân loại và đánh giá mức độ rủi ro tối thiểu theo: nhóm khách hàng, hành vi sử dụng của khách hàng, loại giao dịch, hạn mức giao dịch (nếu có) và tuân thủ các quy định của pháp luật liên quan. Trên cơ sở đó, đơn vị cung cấp các hình thức xác nhận giao dịch phù hợp cho khách hàng lựa chọn, tuân thủ tối thiểu các quy định sau:

a) Áp dụng tối thiểu một trong các hình thức xác nhận quy định tại khoản 3, khoản 4, khoản 5, khoản 7, khoản 8, khoản 9 Điều 11 Thông tư này khi thay đổi thông tin định danh khách hàng;

b) Áp dụng tối thiểu một hoặc kết hợp các hình thức xác nhận giao dịch theo quy định tại Thông tư này; Trường hợp văn bản quy phạm pháp luật hướng dẫn về các dịch vụ quy định tại khoản 1 Điều 1 Thông tư này có quy định về hình thức xác nhận giao dịch thì thực hiện theo văn bản quy phạm pháp luật đó;

c) Đối với giao dịch gồm nhiều bước, phải thực hiện xác nhận giao dịch tại bước phê duyệt cuối cùng.

4. Thực hiện kiểm tra, đánh giá an toàn, bảo mật hệ thống Online Banking định kỳ hàng năm.

5. Thường xuyên nhận dạng rủi ro, nguy cơ gây ra rủi ro và xác định nguyên nhân gây ra rủi ro, kịp thời có biện pháp phòng ngừa, kiểm soát và xử lý rủi ro trong cung cấp dịch vụ Online Banking.

6. Các trang thiết bị hạ tầng kỹ thuật công nghệ thông tin cung cấp dịch vụ Online Banking phải có bản quyền, nguồn gốc, xuất xứ rõ ràng. Với các trang thiết bị sắp hết vòng đời sản phẩm và sẽ không được nhà sản xuất tiếp tục hỗ trợ, đơn vị phải có kế hoạch nâng cấp, thay thế theo thông báo của nhà sản xuất, bảo đảm các trang thiết bị hạ tầng có khả năng cài đặt phiên bản phần mềm mới. Trong thời gian chưa nâng cấp, thay thế, đơn vị phải có biện pháp tăng cường bảo đảm an toàn, bảo mật hệ thống Online Banking.

7. Đối với các hệ thống cung cấp dịch vụ cổng thanh toán điện tử, dịch vụ hỗ trợ thu hộ, chi hộ, không phải tuân thủ các quy định tại khoản 7, khoản 9, khoản 10 Điều 7 và Mục 2 Chương II Thông tư này.

8. Hệ thống Online Banking chỉ được hoạt động cung cấp dịch vụ cho khách hàng khi bảo đảm an toàn, bảo mật theo quy định của Thông tư này và các quy định của pháp luật liên quan.

Chương II

CÁC QUY ĐỊNH CỤ THỂ

Mục 1. HẠ TẦNG KỸ THUẬT CỦA HỆ THỐNG ONLINE BANKING

Điều 4. Hệ thống mạng, truyền thông và an toàn, bảo mật

Đơn vị phải thiết lập hệ thống mạng, truyền thông và an toàn, bảo mật đạt yêu cầu tối thiểu sau:

1. Có các giải pháp an toàn, bảo mật tối thiểu gồm:

a) Tường lửa ứng dụng hoặc giải pháp bảo vệ có tính năng tương đương;

b) Tường lửa cơ sở dữ liệu hoặc giải pháp bảo vệ có tính năng tương đương;

c) Giải pháp phòng, chống tấn công từ chối dịch vụ (DoS – Denial of Service attack), tấn công từ chối dịch vụ phân tán (DDoS - Distributed Denial of Service attack) đối với các hệ thống cung cấp dịch vụ trực tiếp trên Internet;

d) Hệ thống quản lý và phân tích sự kiện an toàn thông tin.

2. Thông tin khách hàng (thông tin nhận biết khách hàng, thông tin giao dịch của khách hàng) không được lưu trữ tại phân vùng kết nối Internet và phân vùng trung gian giữa mạng nội bộ và mạng Internet (phân vùng DMZ).

3. Thiết lập chính sách hạn chế tối đa các dịch vụ, cổng kết nối vào hệ thống Online Banking.

4. Kết nối từ bên ngoài mạng nội bộ vào hệ thống Online Banking để quản trị chỉ được thực hiện trong trường hợp không thể kết nối từ mạng nội bộ và bảo đảm an toàn, tuân thủ các quy định sau:

a) Phải được cấp có thẩm quyền phê duyệt sau khi xem xét mục đích, cách thức kết nối;

b) Phải có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn như sử dụng mạng riêng ảo hoặc phương án tương đương;

c) Thiết bị kết nối phải được cài đặt các phần mềm bảo đảm an toàn, bảo mật;

d) Phải áp dụng tối thiểu hai trong các hình thức xác nhận quy định tại khoản 1, khoản 3, khoản 4, khoản 7, khoản 8, khoản 9 Điều 11 Thông tư này khi đăng nhập hệ thống;

đ) Sử dụng giao thức truyền thông được mã hóa an toàn và không lưu mã khóa bí mật tại các phần mềm tiện ích.

5. Đường truyền kết nối mạng cung cấp dịch vụ phải bảo đảm tính sẵn sàng cao và khả năng cung cấp dịch vụ liên tục.

Điều 5. Hệ thống máy chủ và phần mềm hệ thống

1. Yêu cầu đối với máy chủ:

a) Hiệu năng sử dụng tài nguyên máy chủ bao gồm: bộ xử lý trung tâm (CPU), bộ nhớ trong (RAM), thiết bị lưu trữ dữ liệu, thiết bị truy xuất dữ liệu khi lưu trữ hoặc truyền nhận, trung bình hàng tháng tối đa 80% công suất thiết kế;

b) Hệ thống Online Banking phải có máy chủ dự phòng bảo đảm tính sẵn sàng cao;

c) Tách biệt về lô-gíc hoặc vật lý với các máy chủ hoạt động nghiệp vụ khác;

d) Phải được kiểm tra, nâng cao mức độ an toàn, bảo mật (hardening) cho hệ điều hành, cập nhật các bản vá lỗi thường xuyên.

2. Đơn vị phải lập danh mục các phần mềm được phép cài đặt trên máy chủ. Định kỳ tối thiểu 06 tháng một lần cập nhật, kiểm tra, bảo đảm tuân thủ danh mục này.

Điều 6. Hệ quản trị cơ sở dữ liệu

1. Hệ quản trị cơ sở dữ liệu phải có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu.

2. Hệ thống Online Banking phải có cơ sở dữ liệu dự phòng thảm họa, có khả năng thay thế cơ sở dữ liệu chính và bảo đảm đầy đủ, toàn vẹn dữ liệu giao dịch của khách hàng.

3. Hệ quản trị cơ sở dữ liệu phải được kiểm tra, nâng cao mức độ an toàn, bảo mật (hardening) và cập nhật các bản vá lỗi thường xuyên.

4. Đơn vị phải có biện pháp giám sát, ghi nhật ký truy cập cơ sở dữ liệu và các thao tác khi truy cập cơ sở dữ liệu.

Điều 7. Phần mềm ứng dụng Online Banking

1. Các yêu cầu về an toàn, bảo mật phải được xác định trước khi phát triển phần mềm và tổ chức, triển khai trong quá trình phát triển (phân tích, thiết kế, xây dựng, kiểm thử), vận hành chính thức và duy trì hoạt động phần mềm. Các hồ sơ, tài liệu về an toàn, bảo mật của phần mềm phải được hệ thống hóa, lưu trữ, cập nhật đồng bộ khi hệ thống có thay đổi và kiểm soát chặt chẽ, hạn chế tiếp cận.

2. Đơn vị phải kiểm soát mã nguồn phần mềm với các yêu cầu tối thiểu:

a) Đối với mã nguồn phần mềm do đơn vị tự phát triển:

(i) Định kỳ hoặc khi có thay đổi phần mềm ứng dụng, đơn vị phải kiểm tra mã nguồn nhằm loại trừ các đoạn mã độc hại, các lỗ hổng bảo mật. Nhân sự thực hiện kiểm tra phải độc lập với nhân sự phát triển mã nguồn phần mềm;

(ii) Chỉ định cụ thể các cá nhân chịu trách nhiệm quản lý mã nguồn của phần mềm ứng dụng Online Banking;

(iii) Mã nguồn phải được lưu trữ an toàn tại ít nhất hai địa điểm tách biệt về địa lý và có biện pháp bảo vệ tính toàn vẹn của mã nguồn.

b) Trường hợp mã nguồn phần mềm thuê ngoài gia công (outsourced software):

(i) Đơn vị phải yêu cầu bên cung cấp ký cam kết mã nguồn phần mềm là hợp pháp, không giả mạo; cam kết thực hiện các thoả thuận về việc chỉnh sửa mã nguồn khi bảo hành, bảo trì phần mềm;

(ii) Trường hợp được bàn giao mã nguồn, trước khi nghiệm thu bàn giao mã nguồn phần mềm, đơn vị yêu cầu bên cung cấp phải kiểm tra, xử lý, khắc phục các lỗ hổng bảo mật trong mã nguồn. Sau khi mã nguồn được bàn giao, đơn vị thực hiện theo quy định tại điểm a khoản này;

(iii) Trường hợp không được bàn giao mã nguồn, khi ký nghiệm thu sản phẩm, đơn vị phải yêu cầu bên cung cấp thực hiện dò quét, loại bỏ các đoạn mã độc hại và ký cam kết không có các đoạn mã độc hại trong phần mềm ứng dụng.

3. Phần mềm ứng dụng Online Banking phải được kiểm tra, thử nghiệm trước khi vận hành chính thức đáp ứng các yêu cầu tối thiểu sau:

a) Lập và phê duyệt kế hoạch, kịch bản thử nghiệm phần mềm ứng dụng Online Banking, trong đó nêu rõ các điều kiện về tính an toàn, bảo mật phải được đáp ứng;

b) Phát hiện và loại trừ các lỗi, các gian lận có thể xảy ra khi nhập số liệu đầu vào;

c) Đánh giá, dò quét phát hiện lỗ hổng, điểm yếu về mặt kỹ thuật. Đánh giá khả năng phòng, chống các kiểu tấn công bao gồm nhưng không giới hạn: Injection (SQL, Xpath, LDAP), Cross-site Scripting (XSS), Cross-site Request Forgery (XSRF), Server-Side Request Forgery (SSRS), Brute-Force và các loại lỗi bảo mật như: lỗi kiểm soát truy cập; lỗi nhận dạng và xác thực; lỗi mã hóa; lỗi thiết kế, cấu hình không an toàn; lỗi ghi nhật ký và giám sát bảo mật;

d) Ghi lại các lỗi và quá trình xử lý lỗi, đặc biệt là các lỗi về an toàn, bảo mật trong các báo cáo về kiểm tra thử nghiệm;

đ) Kiểm tra thử nghiệm các tính năng an toàn, bảo mật phải được thực hiện

trên các trình duyệt phổ biến (áp dụng đối với phần mềm ứng dụng Online Banking cung cấp qua nền tảng web) và các phần mềm hệ điều hành của thiết bị di động (áp dụng đối với phần mềm ứng dụng Mobile Banking); có cơ chế kiểm tra, thông báo tức thời cho khách hàng khi sử dụng ứng dụng trên các trình duyệt, phiên bản phần mềm hệ điều hành của thiết bị di động đã được kiểm tra và thử nghiệm an toàn.

4. Trước khi triển khai phần mềm ứng dụng Online Banking mới, đơn vị phải đánh giá những rủi ro của quá trình triển khai đối với hoạt động nghiệp vụ, các hệ thống công nghệ thông tin liên quan và lập, triển khai các phương án hạn chế, khắc phục rủi ro.

5. Đơn vị thực hiện quản lý thay đổi phiên bản phần mềm ứng dụng Online Banking đáp ứng các yêu cầu sau:

a) Xây dựng tài liệu phân tích đánh giá tác động của việc thay đổi đối với hệ thống hiện tại, các hệ thống có liên quan khác của đơn vị và được cấp có thẩm quyền phê duyệt trước khi thực hiện;

b) Các phiên bản phần mềm bao gồm cả mã nguồn do đơn vị tự phát phiển hoặc do bên cung cấp bàn giao cần được quản lý tập trung, lưu trữ, bảo mật và có cơ chế phân quyền cho từng thành viên, ghi nhật ký trong việc thao tác với các tập tin;

c) Thông tin về các phiên bản (thời gian cập nhật, người cập nhật, hướng dẫn cập nhật và các thông tin liên quan khác của phiên bản) phải được lưu trữ;

d) Việc nâng cấp phiên bản phải căn cứ trên kết quả thử nghiệm và được cấp có thẩm quyền phê duyệt.

6. Các chức năng bắt buộc của phần mềm ứng dụng Online Banking:

a) Toàn bộ dữ liệu khi truyền trên môi trường mạng hoặc dữ liệu trao đổi giữa phần mềm ứng dụng Online Banking với các trang thiết bị liên quan được áp dụng cơ chế mã hóa điểm đầu đến điểm cuối;

b) Bảo đảm tính toàn vẹn của dữ liệu giao dịch, mọi sửa đổi trái phép phải được phát hiện, cảnh báo, ngăn chặn hoặc có biện pháp xử lý phù hợp để bảo đảm sự chính xác của dữ liệu giao dịch trong quá trình thực hiện giao dịch, lưu trữ dữ liệu;

c) Kiểm soát phiên giao dịch: hệ thống có cơ chế tự động ngắt phiên giao dịch khi người sử dụng không thao tác trong một khoảng thời gian do đơn vị quy định hoặc áp dụng các biện pháp bảo vệ khác;

d) Có chức năng che giấu đối với việc hiển thị các mã khóa bí mật, mã PIN dùng để đăng nhập vào hệ thống;

đ) Có chức năng chống đăng nhập tự động;

e) Trong trường hợp tài khoản giao dịch điện tử quy định tại khoản 1 Điều 9 Thông tư này sử dụng mã PIN hoặc mã khóa bí mật làm hình thức xác nhận, phần mềm ứng dụng Online Banking phải có các chức năng kiểm soát mã PIN và mã khóa bí mật:

(i) Yêu cầu khách hàng thay đổi mã PIN hoặc mã khóa bí mật trong trường hợp khách hàng được cấp phát mã PIN hoặc mã khóa bí mật mặc định lần đầu;

(ii) Thông báo cho khách hàng khi mã PIN hoặc mã khóa bí mật sắp hết hiệu lực sử dụng;

(iii) Hủy hiệu lực của mã PIN hoặc mã khóa bí mật khi hết hạn sử dụng; yêu cầu khách hàng thay đổi mã PIN hoặc mã khóa bí mật đã hết hạn sử dụng khi khách hàng sử dụng mã PIN hoặc mã khóa bí mật để đăng nhập;

(iv) Hủy hiệu lực của mã PIN hoặc mã khóa bí mật trong trường hợp bị nhập sai mã PIN hoặc mã khóa bí mật liên tiếp quá số lần do đơn vị quy định (nhưng không quá 10 lần) và thông báo cho khách hàng;

(v) Đơn vị chỉ cấp phát lại mã PIN hoặc mã khóa bí mật khi khách hàng yêu cầu và phải kiểm tra, nhận biết khách hàng trước khi thực hiện cấp phát lại, bảo đảm chống gian lận, giả mạo.

g) Đối với khách hàng là tổ chức, phần mềm ứng dụng được thiết kế để bảo đảm việc thực hiện giao dịch thanh toán trực tuyến bao gồm tối thiểu hai bước: tạo lập và phê duyệt giao dịch. Trong trường hợp khách hàng là hộ kinh doanh hoặc doanh nghiệp siêu nhỏ áp dụng chế độ kế toán đơn giản, việc thực hiện giao dịch không bắt buộc tách biệt hai bước tạo lập và phê duyệt giao dịch;

h) Có chức năng thông báo việc đăng nhập lần đầu phần mềm ứng dụng Online Banking hoặc việc đăng nhập phần mềm ứng dụng Online Banking trên thiết bị khác với thiết bị thực hiện đăng nhập phần mềm ứng dụng Online Banking lần gần nhất qua SMS hoặc các kênh khác do khách hàng đăng ký (điện thoại, thư điện tử...), ngoại trừ trường hợp khách hàng tổ chức: đăng nhập trên các thiết bị đã đăng ký sử dụng dịch vụ; hoặc đăng nhập sử dụng tối thiểu một trong các hình thức xác nhận quy định tại khoản 3, khoản 4, khoản 5, khoản 7, khoản 8, khoản 9 Điều 11 Thông tư này.

7. Phần mềm ứng dụng Online Banking phải có chức năng lưu trữ trực tuyến thông tin về thiết bị thực hiện các giao dịch của khách hàng, nhật ký (log) giao dịch, nhật ký xác nhận giao dịch tối thiểu trong vòng 03 tháng và sao lưu tối thiểu 01 năm, trong đó gồm:

a) Thông tin định danh về thiết bị:

(i) Đối với thiết bị di động: thông tin để định danh duy nhất thiết bị (ví dụ như: số IMEI hoặc Serial hoặc WLAN MAC hoặc Android ID hoặc thông tin định danh khác);

(ii) Đối với máy tính: thông tin để định danh duy nhất máy tính (ví dụ như địa chỉ MAC hoặc kết hợp các thông tin liên quan đến máy tính để có thể định danh duy nhất máy tính).

b) Nhật ký (log) giao dịch tối thiểu gồm: mã giao dịch, mã khách hàng, thời gian khởi tạo giao dịch, loại giao dịch, giá trị giao dịch (nếu có);

c) Nhật ký (log) xác nhận giao dịch tối thiểu gồm: hình thức xác nhận giao dịch, thời gian xác nhận giao dịch. Trường hợp xác nhận giao dịch bằng hình thức khớp đúng thông tin sinh trắc học, đơn vị thực hiện lưu trữ thông tin sinh trắc học của khách hàng khi thực hiện giao dịch đối với tối thiểu 10 giao dịch gần nhất của khách hàng đó.

8. Các yêu cầu đối với phương thức xử lý xuyên suốt:

a) Đơn vị chỉ cung cấp dịch vụ Online Banking bằng phương thức xử lý xuyên suốt cho khách hàng là tổ chức. Đơn vị có trách nhiệm lựa chọn, thẩm định, giám sát, quản lý và có thỏa thuận với khách hàng khi cung cấp dịch vụ Online Banking bằng phương thức xử lý xuyên suốt;

b) Phần mềm ứng dụng Online Banking phải có chức năng xác thực kết nối với phần mềm của khách hàng tổ chức để bảo đảm chống gian lận, giả mạo;

c) Không bắt buộc áp dụng nội dung quy định tại điểm c, điểm đ, điểm e, điểm g, điểm h khoản 6 và điểm a khoản 7 Điều này.

9. Tổ chức phát hành thẻ có cung cấp dịch vụ thanh toán trực tuyến sử dụng thẻ ngân hàng, phải có phần mềm ứng dụng Online Banking có tối thiểu các tính năng sau:

a) Cho phép hoặc không cho phép thanh toán trực tuyến;

b) Thiết lập hạn mức thanh toán trực tuyến sử dụng thẻ ngân hàng trong ngày;

c) Cho phép hoặc không cho phép thanh toán ở nước ngoài tại thiết bị chấp nhận thẻ tại điểm bán, máy giao dịch tự động;

d) Cho phép khách hàng đăng ký lựa chọn việc chủ động thực hiện xác nhận hoặc đồng ý để tổ chức phát hành thẻ thực hiện xác nhận đối với tất cả hoặc một phần giao dịch thanh toán trực tuyến sử dụng thẻ ngân hàng (giao dịch thanh toán thẻ trực tuyến) trong trường hợp sử dụng hình thức xác nhận theo quy định tại khoản 10 Điều 11 Thông tư này.

10. Phần mềm ứng dụng Online Banking phải có chức năng thông báo cho

khách hàng về các giao dịch phát sinh qua tin nhắn SMS hoặc thư điện tử hoặc phần mềm ứng dụng Mobile Banking hoặc các kênh liên lạc khác do khách hàng đăng ký.

Điều 8. Phần mềm ứng dụng Mobile Banking

Phần mềm ứng dụng Mobile Banking do đơn vị cung cấp phải bảo đảm tuân thủ các quy định tại Điều 7 Thông tư này và các yêu cầu sau:

1. Phải được đăng ký và quản lý tại kho ứng dụng chính thức của hãng cung cấp hệ điều hành cho thiết bị di động và hướng dẫn cài đặt rõ ràng trên trang tin điện tử đơn vị để khách hàng tải và cài đặt phần mềm ứng dụng Mobile Banking. Trong trường hợp vì lý do khách quan mà phần mềm ứng dụng Mobile Banking không được đăng ký và quản lý tại kho ứng dụng chính thức của hãng cung cấp hệ điều hành cho thiết bị di động, đơn vị phải có phương thức hướng dẫn, thông báo, hỗ trợ cài đặt phần mềm ứng dụng Mobile Banking bảo đảm an toàn, bảo mật cho khách hàng và báo cáo về Ngân hàng Nhà nước (Cục Công nghệ thông tin) trước khi cung cấp dịch vụ.

2. Phải được áp dụng các biện pháp bảo vệ để hạn chế dịch ngược mã nguồn.

3. Có biện pháp bảo vệ, chống can thiệp vào luồng trao đổi dữ liệu trên ứng dụng Mobile Banking và giữa ứng dụng Mobile Banking với máy chủ cung cấp dịch vụ Online Banking.

4. Triển khai các giải pháp nhằm phòng, chống, phát hiện các hành vi can thiệp trái phép vào ứng dụng Mobile Banking đã cài đặt trong thiết bị di động của khách hàng.

5. Không cho phép chức năng ghi nhớ mã khóa bí mật truy cập.

6. Đối với khách hàng cá nhân, phải có chức năng kiểm tra khách hàng khi khách hàng truy cập lần đầu hoặc khi khách hàng truy cập trên thiết bị khác với thiết bị đã truy cập phần mềm ứng dụng Mobile Banking lần gần nhất. Việc kiểm tra khách hàng tối thiểu bao gồm:

a) Khớp đúng SMS OTP hoặc Voice OTP thông qua số điện thoại đã được khách hàng đăng ký hoặc Soft OTP/Token OTP;

b) Khớp đúng thông tin sinh trắc học theo quy định tại khoản 5 Điều 11 Thông tư này trong trường hợp văn bản pháp luật chuyên ngành liên quan đến dịch vụ cung cấp trên phần mềm ứng dụng Mobile Banking có quy định thu thập, lưu trữ thông tin sinh trắc học của khách hàng.

Mục 2. XÁC NHẬN GIAO DỊCH ĐIỆN TỬ THÔNG QUA HỆ THỐNG ONLINE BANKING

Điều 9. Truy cập phần mềm ứng dụng Online Banking

1. Khách hàng đăng ký sử dụng phần mềm ứng dụng Online Banking phải được đơn vị nhận biết khách hàng và cấp tài khoản giao dịch điện tử. Tài khoản giao dịch điện tử gồm tên đăng nhập và tối thiểu một trong các hình thức xác nhận quy định tại khoản 1, khoản 2, khoản 3, khoản 4, khoản 5, khoản 6, khoản 7, khoản 8, khoản 9 Điều 11 Thông tư này.

2. Khách hàng truy cập phần mềm ứng dụng Online Banking bằng tài khoản giao dịch điện tử do đơn vị cấp hoặc truy cập bằng hình thức đăng nhập một lần (Single Sign On) thông qua tài khoản giao dịch điện tử của hệ thống thông tin khác đã được đơn vị tích hợp và theo đăng ký của khách hàng.

Điều 10. Xác nhận giao dịch

1. Đối với giao dịch thanh toán trực tuyến:

a) Đối với giao dịch thanh toán sử dụng tài khoản thanh toán hoặc ví điện tử hoặc giao dịch chuyển tiền từ thẻ ghi nợ, thẻ trả trước định danh, đơn vị thực hiện phân loại giao dịch theo các nhóm loại hình giao dịch quy định tại Phụ lục 01 ban hành kèm theo Thông tư này và áp dụng hình thức xác nhận quy định tại Phụ lục 02 ban hành kèm theo Thông tư này, trừ quy định tại điểm b, điểm c, điểm d và điểm đ khoản này;

b) Đối với giao dịch thanh toán thực hiện bằng phương thức xử lý xuyên suốt, đơn vị thực hiện xác nhận giao dịch tối thiểu bằng một trong các hình thức xác nhận quy định tại khoản 7, khoản 8, khoản 9 Điều 11 Thông tư này;

c) Đối với các giao dịch thanh toán thẻ trực tuyến (không bao gồm giao dịch chuyển tiền), đơn vị thực hiện phân loại giao dịch theo các nhóm loại hình giao dịch quy định tại Phụ lục 03 ban hành kèm theo Thông tư này và áp dụng các hình thức xác nhận quy định tại Phụ lục 04 ban hành kèm theo Thông tư này;

d) Đối với các giao dịch mà đơn vị chủ động trích Nợ tài khoản thanh toán, chủ động trích Nợ ví điện tử, chủ động thanh toán từ thẻ của khách hàng theo thỏa thuận với khách hàng, không phải áp dụng xác nhận giao dịch quy định tại điểm a, điểm c khoản 1 Điều này;

đ) Đối với các giao dịch thanh toán trực tuyến trên Cổng Dịch vụ công quốc gia, nộp tiền vào ngân sách nhà nước, không bắt buộc phải áp dụng xác nhận giao dịch quy định tại điểm a, điểm c khoản 1 Điều này.

2. Đối với giao dịch đăng ký tự động trích Nợ tài khoản thanh toán, tự động trích Nợ ví điện tử, tự động thanh toán từ thẻ của khách hàng, đơn vị áp dụng tối thiểu một trong các hình thức xác nhận quy định tại khoản 3, khoản 4, khoản 5, khoản 7, khoản 8, khoản 9 Điều 11 Thông tư này.

3. Đối với các giao dịch khác, ngoài giao dịch quy định tại khoản 1, khoản 2 Điều này, trên cơ sở đánh giá rủi ro và tuân thủ quy định của pháp luật có liên

quan, đơn vị lựa chọn hình thức xác nhận phù hợp theo quy định tại Điều 11 Thông tư này để cung cấp cho khách hàng đăng ký sử dụng và chịu trách nhiệm với việc lựa chọn này.

4. Trường hợp khách hàng là người khuyết tật, đơn vị căn cứ điều kiện, khả năng cung ứng của đơn vị mình để cung cấp và hướng dẫn khách hàng là người khuyết tật lựa chọn hình thức xác nhận phù hợp, không bắt buộc áp dụng quy định tại khoản 1, khoản 2, khoản 3 Điều này, nhưng phải bảo đảm kiểm tra, xác nhận được sự chấp thuận của khách hàng khi thực hiện giao dịch theo quy định của pháp luật về giao dịch điện tử và Thông tư này.

Điều 11. Các hình thức xác nhận

1. Hình thức xác nhận bằng *mã khóa bí mật* (Password): khách hàng sử dụng mã khóa bí mật là một chuỗi ký tự để xác nhận quyền truy cập của khách hàng vào hệ thống thông tin, ứng dụng, dịch vụ hoặc xác nhận khách hàng thực hiện giao dịch. Hình thức xác nhận bằng mã khóa bí mật phải đáp ứng yêu cầu:

a) Mã khóa bí mật có độ dài tối thiểu 08 ký tự và cấu tạo bao gồm tối thiểu các ký tự: số, chữ hoa, chữ thường;

b) Thời gian hiệu lực của mã khóa bí mật tối đa 12 tháng, đối với mã khóa bí mật được cấp phát mặc định lần đầu: thời gian hiệu lực tối đa là 30 ngày.

2. Hình thức xác nhận bằng *mã PIN* (Personal Identification Number) là hình thức xác nhận bằng mã khóa bí mật trong đó mã khóa bí mật được tạo từ một chuỗi các chữ số. Hình thức xác nhận bằng mã PIN (trừ trường hợp mã PIN gắn với thẻ vật lý) phải đáp ứng yêu cầu:

a) Mã PIN có độ dài tối thiểu 06 ký tự;

b) Thời gian hiệu lực của mã PIN tối đa 12 tháng, đối với mã PIN được cấp phát mặc định lần đầu: thời gian hiệu lực tối đa là 30 ngày.

3. Hình thức xác nhận bằng *mã khóa bí mật dùng một lần* (One Time Password - OTP) là hình thức xác nhận bằng mã khóa bí mật trong đó mã khóa bí mật có giá trị sử dụng một lần và có hiệu lực trong một khoảng thời gian nhất định, bao gồm các hình thức sau:

a) *SMS OTP* là hình thức xác nhận thông qua mã OTP được gửi qua tin nhắn SMS (Short Message Services) hoặc tin nhắn thông qua dịch vụ viễn thông cơ bản trên Internet. SMS OTP phải đáp ứng yêu cầu:

(i) OTP gửi tới khách hàng phải kèm thông tin thông báo để khách hàng nhận biết được mục đích của OTP;

(ii) OTP có hiệu lực tối đa 05 phút.

b) *Voice OTP* là hình thức xác nhận thông qua mã OTP được gửi qua cuộc

gọi thoại hoặc cuộc gọi thông qua dịch vụ viễn thông cơ bản trên Internet. Voice OTP phải đáp ứng yêu cầu:

(i) OTP gửi tới khách hàng phải kèm thông tin thông báo để khách hàng nhận biết được mục đích của OTP;

(ii) OTP có hiệu lực tối đa 03 phút.

c) *Email OTP* là hình thức xác nhận thông qua mã OTP được gửi qua thư điện tử. Email OTP phải đáp ứng yêu cầu:

(i) OTP gửi tới khách hàng phải kèm thông tin thông báo để khách hàng nhận biết được mục đích của OTP;

(ii) OTP có hiệu lực tối đa 05 phút.

d) *Thẻ ma trận OTP* là hình thức xác nhận thông qua mã OTP được xác định từ một bảng 2 chiều (dòng, cột), tương ứng với mỗi dòng, cột là một mã OTP. Thẻ ma trận OTP phải đáp ứng yêu cầu:

(i) Thẻ ma trận OTP có thời hạn sử dụng tối đa 01 năm kể từ ngày đăng ký thẻ;

(ii) OTP có hiệu lực tối đa 02 phút.

đ) *Soft OTP* là hình thức xác nhận thông qua mã OTP được tạo bởi phần mềm cài đặt trên thiết bị di động của khách hàng, phần mềm Soft OTP có thể là phần mềm độc lập hoặc được tích hợp với phần mềm ứng dụng Mobile Banking.

Soft OTP có 02 loại: (i) *Soft OTP loại cơ bản*: Mã OTP được sinh ngẫu nhiên theo thời gian, đồng bộ với hệ thống Online Banking; (ii) *Soft OTP loại nâng cao*: Mã OTP được tạo kết hợp với mã của từng giao dịch, khi thực hiện giao dịch, hệ thống Online Banking tạo ra một mã giao dịch thông báo cho khách hàng hoặc truyền cho phần mềm Soft OTP, khách hàng hoặc phần mềm Soft OTP tự động nhập mã giao dịch vào phần mềm Soft OTP để phần mềm Soft OTP tạo ra mã OTP.

Soft OTP phải đáp ứng yêu cầu:

(i) Trường hợp phần mềm Soft OTP độc lập với phần mềm ứng dụng Mobile Banking, phải được đơn vị đăng ký, quản lý tại kho ứng dụng chính thức của hãng cung cấp hệ điều hành cho thiết bị di động và hướng dẫn cài đặt rõ ràng trên trang tin điện tử của đơn vị để khách hàng tải và cài đặt phần mềm Soft OTP;

(ii) Phần mềm Soft OTP phải yêu cầu kích hoạt trước khi sử dụng. Mã kích hoạt sử dụng Soft OTP do đơn vị cung cấp cho khách hàng và chỉ được sử dụng để kích hoạt trên một thiết bị di động. Mã kích hoạt phải được thiết lập thời hạn hiệu lực sử dụng;

(iii) Phần mềm Soft OTP phải có chức năng kiểm soát truy cập. Trường hợp truy cập sai liên tiếp quá số lần do đơn vị quy định (nhưng không quá 10 lần), phần mềm Soft OTP phải tự động khóa không cho khách hàng sử dụng tiếp. Đơn vị chỉ mở khóa phần mềm Soft OTP khi khách hàng yêu cầu và phải kiểm tra, nhận biết khách hàng trước khi thực hiện mở khóa, bảo đảm chống gian lận, giả mạo.

(iv) Trường hợp phần mềm Soft OTP độc lập với phần mềm ứng dụng Mobile Banking phải có chức năng kiểm tra khách hàng cá nhân trước khi cho phép khách hàng sử dụng lần đầu hoặc trước khi khách hàng sử dụng trên thiết bị khác với thiết bị sử dụng lần gần nhất. Việc kiểm tra khách hàng tối thiểu bao gồm: (i) khớp đúng SMS OTP hoặc Voice OTP thông qua số điện thoại đã được khách hàng đăng ký, (ii) và khớp đúng thông tin sinh trắc học của khách hàng;

(v) Mã OTP có hiệu lực tối đa 02 phút.

e) *Token OTP* là hình thức xác nhận thông qua mã OTP tạo bởi thiết bị chuyên dụng. Token OTP có 02 loại: (i) *Token OTP loại cơ bản*: Mã OTP được tạo một cách ngẫu nhiên theo thời gian, đồng bộ với hệ thống Online Banking; (ii) *Token OTP loại nâng cao*: Mã OTP được tạo ra kết hợp với mã của từng giao dịch. Khi thực hiện giao dịch, hệ thống Online Banking tạo ra một mã giao dịch thông báo cho khách hàng, khách hàng nhập mã giao dịch vào Token OTP để thiết bị tạo ra mã OTP. Token OTP có hiệu lực tối đa 02 phút.

4. Hình thức xác nhận *hai kênh* là hình thức xác nhận khi khách hàng thực hiện giao dịch, hệ thống Online Banking sẽ gửi thông tin yêu cầu xác nhận giao dịch đến thiết bị di động của khách hàng qua cuộc gọi thoại hoặc cuộc gọi thông qua dịch vụ viễn thông cơ bản trên Internet hoặc qua mã tin nhắn nhanh USSD (Unstructured Supplementary Service Data) hoặc qua phần mềm chuyên dụng, khách hàng phản hồi trực tiếp qua kênh đã kết nối để xác nhận hoặc không xác nhận thực hiện giao dịch. Yêu cầu xác nhận của hình thức xác nhận hai kênh có hiệu lực tối đa 05 phút.

5. Hình thức xác nhận *khớp đúng thông tin sinh trắc học* là việc đối chiếu, so sánh để bảo đảm trùng khớp thông tin sinh trắc học của khách hàng đang thực hiện giao dịch với thông tin sinh trắc học của khách hàng đã thu thập, lưu trữ tại đơn vị theo quy định của Thống đốc Ngân hàng Nhà nước. Hình thức khớp đúng thông tin sinh trắc học phải đáp ứng tối thiểu yêu cầu:

a) Trường hợp áp dụng hình thức khớp đúng thông tin sinh trắc học sử dụng khuôn mặt:

(i) Có độ chính xác được xác định theo tiêu chuẩn quốc tế như sau (hoặc tương đương): Có tỷ lệ từ chối sai < 5% với tỷ lệ chấp nhận sai < 0,01% theo tiêu chuẩn FIDO Biometric Requirement (áp dụng đối với tập mẫu tối thiểu 10.000

mẫu);

(ii) Có khả năng phát hiện tấn công giả mạo thông tin sinh trắc học của vật thể sống (Presentation Attack Detection - PAD) dựa trên các tiêu chuẩn quốc tế (như NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management hoặc ISO 30107 - Biometric presentation attack detection hoặc FIDO Biometric Requirements) để phòng, chống gian lận, giả mạo khách hàng qua hình ảnh, video, mặt nạ 3D.

b) Trường hợp áp dụng các hình thức khớp đúng thông tin sinh trắc học khác, phải bảo đảm phòng, chống gian lận, giả mạo khách hàng theo tiêu chuẩn tương đương;

c) Giải pháp phát hiện tấn công giả mạo thông tin sinh trắc học của vật thể sống (Presentation Attack Detection - PAD) theo quy định tại điểm a khoản này do đơn vị tự triển khai hoặc sử dụng của bên thứ ba cung cấp phải được cấp chứng nhận của tổ chức/phòng thí nghiệm sinh trắc học được Liên minh FIDO (FIDO Alliance) công nhận;

d) Trường hợp khách hàng xác nhận bằng hình thức khớp đúng thông tin sinh trắc học quá số lần sai liên tiếp do đơn vị quy định (nhưng không quá 10 lần): khóa chức năng thực hiện xác nhận giao dịch bằng hình thức khớp đúng thông tin sinh trắc học, chỉ mở khóa khi khách hàng yêu cầu và phải kiểm tra khách hàng trước khi thực hiện, bảo đảm chống gian lận, giả mạo;

đ) Thời gian thực hiện khớp đúng thông tin sinh trắc học tối đa 03 phút.

6. Hình thức xác nhận *khớp đúng thông tin sinh trắc học thiết bị* là việc đối chiếu, so sánh để bảo đảm trùng khớp thông tin sinh trắc học của khách hàng đang thực hiện giao dịch với thông tin sinh trắc học của khách hàng đã lưu trữ trên thiết bị di động của khách hàng. Hình thức khớp đúng thông tin sinh trắc học thiết bị phải đáp ứng yêu cầu:

a) Chỉ cho phép kích hoạt sử dụng sau khi có sự đồng ý của khách hàng và khách hàng đã thực hiện ít nhất một giao dịch thành công bằng hình thức xác nhận khác;

b) Thời gian thực hiện khớp đúng thông tin sinh trắc học tối đa 02 phút.

7. Hình thức xác nhận *FIDO* (Fast IDentity Online) là hình thức xác nhận theo tiêu chuẩn về xác nhận giao dịch sử dụng thuật toán khóa không đối xứng (gồm khóa bí mật và khóa công khai, trong đó khóa bí mật được dùng để ký số và khóa công khai được dùng để kiểm tra chữ ký số) do Liên minh FIDO (FIDO Alliance) ban hành. Hình thức xác nhận FIDO phải đáp ứng yêu cầu:

a) Khóa bí mật được lưu giữ an toàn trên thiết bị của khách hàng. Khách hàng sử dụng hình thức xác nhận bằng mã PIN hoặc khớp đúng thông tin sinh trắc

học thiết bị để truy cập, sử dụng khóa bí mật khi thực hiện giao dịch;

b) Khóa công khai được lưu trữ an toàn tại đơn vị và được liên kết với tài khoản giao dịch điện tử của khách hàng;

c) Giải pháp do đơn vị tự triển khai hoặc sử dụng của bên thứ ba cung cấp phải được cấp chứng nhận của tổ chức được Liên minh FIDO (FIDO Alliance) công nhận.

8. Hình thức xác nhận bằng *chữ ký điện tử* theo quy định của pháp luật về chữ ký điện tử (không bao gồm chữ ký điện tử an toàn quy định tại khoản 9 Điều này).

9. Hình thức xác nhận bằng *chữ ký điện tử an toàn* là hình thức xác nhận bằng chữ ký điện tử, trong đó chữ ký điện tử là chữ ký điện tử chuyên dùng bảo đảm an toàn hoặc chữ ký số hoặc chữ ký điện tử nước ngoài được công nhận tại Việt Nam theo quy định của pháp luật về chữ ký điện tử.

10. Hình thức xác nhận trên cơ sở đánh giá rủi ro đối với giao dịch thanh toán thẻ trực tuyến theo tiêu chuẩn EMV 3-D Secure (sau đây gọi tắt là *hình thức xác nhận EMV 3DS*). Hình thức xác nhận EMV 3DS phải đáp ứng yêu cầu: Tổ chức phát hành thẻ, tổ chức thanh toán thẻ và đơn vị chấp nhận thẻ phải triển khai tiêu chuẩn EMV 3-D Secure.

11. Hình thức xác nhận thông qua *các thao tác thể hiện sự xác nhận* của khách hàng đối với thông điệp dữ liệu khi thực hiện giao dịch như bấm chấp nhận, phê duyệt, gửi hoặc các hoạt động tương tự trên phần mềm ứng dụng Online Banking. Hình thức xác nhận thông qua các thao tác thể hiện sự xác nhận của khách hàng đối với thông điệp dữ liệu khi thực hiện giao dịch phải đáp ứng yêu cầu:

a) Các thao tác xác nhận phải được lưu trữ nhật ký (log) để có thể truy vấn được thông tin liên quan đến các thao tác xác nhận này;

b) Khách hàng là tổ chức và đã thực hiện đăng nhập phần mềm ứng dụng Online Banking sử dụng hình thức xác nhận theo quy định tại Điều này trừ khoản 1, khoản 2, khoản 6, khoản 10.

Mục 3. QUẢN LÝ VẬN HÀNH

Điều 12. Quản lý nhân sự quản trị, vận hành hệ thống Online Banking

1. Đơn vị phải phân công nhân sự giám sát, theo dõi hoạt động của hệ thống Online Banking, phát hiện và xử lý các sự cố kỹ thuật, các cuộc tấn công mạng.

2. Đơn vị phải phân công nhân sự tiếp nhận thông tin, hỗ trợ khách hàng, kịp thời liên lạc với khách hàng khi phát hiện các giao dịch bất thường.

3. Nhân sự quản trị, giám sát và vận hành hệ thống Online Banking phải tham gia các khóa đào tạo cập nhật kiến thức an toàn, bảo mật hằng năm.

4. Việc cấp phát, phân quyền tài khoản quản trị hệ thống Online Banking phải được theo dõi, giám sát bởi bộ phận độc lập với bộ phận cấp phát tài khoản.

Điều 13. Quản lý hoạt động của môi trường vận hành hệ thống Online Banking

1. Đơn vị không cài đặt, lưu trữ phần mềm phát triển ứng dụng, mã nguồn trên môi trường vận hành.

2. Hoạt động quản trị, giám sát và vận hành phải đáp ứng các yêu cầu sau:

a) Máy tính của nhân sự quản trị, giám sát và vận hành chỉ được cài đặt các phần mềm được phép sử dụng và phải được cài đặt phần mềm phòng chống mã độc, cập nhật thường xuyên các mẫu nhận diện mã độc và không cho phép tự vô hiệu hóa phần mềm phòng chống mã độc;

b) Việc kết nối quản trị, giám sát và vận hành hệ thống phải qua các máy chủ trung gian hoặc các hệ thống quản trị tập trung an toàn, có kiểm soát, không thực hiện trực tiếp từ máy tính của nhân sự quản trị, giám sát và vận hành;

c) Việc sử dụng tài khoản có quyền quản trị phải được giới hạn trong khoảng thời gian đủ để thực hiện công việc và phải được thu hồi ngay sau khi kết thúc phiên làm việc;

d) Phải có biện pháp giám sát việc sử dụng tài khoản có quyền quản trị, giám sát và vận hành, có cảnh báo khi có tác động bất thường vào cơ sở dữ liệu, ứng dụng.

3. Đơn vị phải thiết lập chính sách đối với các máy tính thực hiện quản trị, giám sát và vận hành hệ thống Online Banking chỉ được phép kết nối đến hệ thống Online Banking hoặc các hệ thống thông tin khác của đơn vị để phục vụ quản trị, giám sát và vận hành.

Điều 14. Quản lý lỗ hổng, điểm yếu về mặt kỹ thuật

Đơn vị phải thực hiện quản lý các lỗ hổng, điểm yếu của hệ thống Online Banking với các nội dung cơ bản sau:

1. Có biện pháp phòng, chống, dò tìm phát hiện các thay đổi trái phép đối với phần mềm ứng dụng Online Banking.

2. Thiết lập cơ chế phát hiện, phòng chống xâm nhập, tấn công mạng vào hệ thống Online Banking.

3. Phối hợp với các đơn vị quản lý nhà nước, các đối tác công nghệ thông tin kịp thời nắm bắt các sự cố, tình huống mất an toàn, bảo mật thông tin để có biện

pháp ngăn chặn kịp thời.

4. Cập nhật thông tin các lỗ hổng bảo mật được công bố có liên quan đến phần mềm hệ thống, hệ quản trị cơ sở dữ liệu và phần mềm ứng dụng theo thông tin từ Hệ thống tính điểm lỗ hổng phổ biến (Common Vulnerability Scoring System version 4 - CVSS v4 hoặc tương đương).

5. Thực hiện dò quét lỗ hổng, điểm yếu của hệ thống Online Banking tối thiểu mỗi năm một lần hoặc khi tiếp nhận được những thông tin liên quan đến lỗ hổng, điểm yếu mới. Đối với thành phần hệ thống kết nối trực tiếp với Internet thực hiện dò quét lỗ hổng, điểm yếu tối thiểu 03 tháng một lần. Đánh giá mức độ tác động, rủi ro của từng lỗ hổng, điểm yếu về mặt kỹ thuật được phát hiện của hệ thống và đưa ra phương án, kế hoạch xử lý.

6. Thực hiện triển khai cập nhật các bản vá bảo mật hoặc các biện pháp phòng ngừa kịp thời căn cứ theo đánh giá mức độ tác động, rủi ro:

a) Đối với lỗ hổng bảo mật được đánh giá ở mức nghiêm trọng: trong vòng 01 ngày đối với thành phần hệ thống kết nối trực tiếp với Internet; trong vòng 01 tháng đối với các thành phần còn lại sau khi lỗ hổng được công bố hoặc phát hiện.

b) Đối với lỗ hổng bảo mật được đánh giá ở mức cao: trong vòng 01 ngày đối với thành phần hệ thống kết nối trực tiếp với Internet; trong vòng 02 tháng đối với các thành phần còn lại sau khi lỗ hổng được công bố hoặc phát hiện.

c) Đối với lỗ hổng bảo mật được đánh giá ở mức trung bình hoặc thấp: thực hiện trong khoảng thời gian do đơn vị tự quyết định.

Điều 15. Hệ thống giám sát, theo dõi hoạt động của hệ thống Online Banking

1. Đơn vị phải thiết lập hệ thống giám sát, theo dõi hoạt động của hệ thống Online Banking. Hệ thống giám sát, theo dõi hoạt động của hệ thống Online Banking phải thu thập đầy đủ nhật ký (log) của các thành phần thuộc hệ thống Online Banking để phát hiện, điều tra các sự kiện bất thường hoặc các hành vi tấn công mạng.

2. Đơn vị phải xây dựng các tiêu chí và phần mềm để cảnh báo các giao dịch bất thường dựa vào thời gian, vị trí địa lý, tần suất giao dịch, số tiền giao dịch (nếu có), số lần đăng nhập sai quá quy định và các dấu hiệu bất thường khác.

Điều 16. Bảo đảm hoạt động liên tục

Đơn vị phải xây dựng hệ thống dự phòng thảm hoạ, quy trình, kịch bản bảo đảm hoạt động liên tục cho hệ thống Online Banking theo quy định của Ngân hàng Nhà nước về bảo đảm an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng. Ngoài ra, đơn vị phải thực hiện:

1. Phân tích, xác định các tình huống có thể gây mất an toàn thông tin và gián đoạn hoạt động của hệ thống Online Banking. Xác định, đánh giá mức độ rủi ro, khả năng có thể xảy ra đối với từng tình huống tối thiểu 06 tháng một lần. Lập danh sách các tình huống có mức độ rủi ro, khả năng có thể xảy ra theo các cấp độ cao, trung bình, chấp nhận được và thấp.

2. Xây dựng phương án bao gồm quy trình, kịch bản xử lý khắc phục các tình huống có mức độ rủi ro, khả năng có thể xảy ra ở cấp độ cao và trung bình theo quy định tại khoản 1 Điều này. Xác định thời gian dừng hoạt động tối đa để phục hồi hệ thống, phục hồi dữ liệu cho phương án xử lý đối với từng tình huống. Tổ chức phổ biến phương án xử lý đến các nhân sự có liên quan để hiểu rõ nhiệm vụ, công việc cần phải thực hiện khi xử lý.

3. Bố trí nguồn nhân lực, tài chính và các phương tiện kỹ thuật để tổ chức diễn tập phương án xử lý với các tình huống có mức độ rủi ro, khả năng có thể xảy ra ở cấp độ cao theo định kỳ tối thiểu 01 năm một lần.

4. Lập kế hoạch và tiến hành diễn tập các biện pháp bảo đảm hoạt động kinh doanh liên tục, lưu giữ các hồ sơ có liên quan và tổ chức đánh giá kết quả diễn tập.

Mục 4. BẢO VỆ QUYỀN LỢI CỦA KHÁCH HÀNG

Điều 17. Thông tin về dịch vụ Online Banking

1. Đơn vị phải công bố thông tin về dịch vụ Online Banking, bảo đảm khách hàng có khả năng tiếp cận được thông tin trước hoặc ngay tại thời điểm đăng ký sử dụng dịch vụ, thông tin công bố tối thiểu gồm có:

a) Cách thức cung cấp dịch vụ, cách thức truy cập dịch vụ Online Banking ứng với từng phương tiện truy cập;

b) Hạn mức giao dịch (nếu có) và các hình thức xác nhận giao dịch;

c) Các trang thiết bị cần thiết để sử dụng dịch vụ, điều kiện với các trang thiết bị được sử dụng;

d) Các rủi ro liên quan đến việc sử dụng dịch vụ Online Banking.

2. Đơn vị phải thông tin cho khách hàng về các điều khoản trong thỏa thuận cung cấp, sử dụng dịch vụ Online Banking, tối thiểu gồm:

a) Quyền lợi và nghĩa vụ của khách hàng sử dụng dịch vụ Online Banking;

b) Các loại dữ liệu của khách hàng mà đơn vị thu thập, mục đích sử dụng dữ liệu của khách hàng và trách nhiệm của đơn vị trong bảo mật dữ liệu của khách hàng theo quy định của pháp luật trừ trường hợp đơn vị và khách hàng đã có thỏa thuận khác về việc bảo vệ dữ liệu khách hàng phù hợp với quy định của pháp luật;

c) Cam kết khả năng bảo đảm hoạt động liên tục của hệ thống Online Banking, tối thiểu gồm: thời gian gián đoạn cung cấp dịch vụ trong một lần, tổng thời gian gián đoạn cung cấp dịch vụ trong một năm trừ các trường hợp bất khả kháng hoặc bảo trì, nâng cấp hệ thống đã được đơn vị thông báo;

d) Các nội dung khác của đơn vị đối với dịch vụ Online Banking (nếu có).

3. Đơn vị không gửi tin nhắn SMS, thư điện tử cho khách hàng có nội dung chứa đường dẫn liên kết (Hyperlink) truy cập các trang tin điện tử, trừ trường hợp theo yêu cầu của khách hàng.

Điều 18. Hướng dẫn khách hàng sử dụng dịch vụ Online Banking

1. Đơn vị phải xây dựng quy trình, tài liệu hướng dẫn cài đặt, sử dụng các phần mềm, ứng dụng, thiết bị thực hiện các giao dịch điện tử và cung cấp, hướng dẫn khách hàng sử dụng các quy trình, tài liệu này.

2. Đơn vị phải hướng dẫn khách hàng thực hiện các biện pháp bảo đảm an toàn, bảo mật khi sử dụng dịch vụ Online Banking, tối thiểu gồm các nội dung sau:

a) Bảo vệ bí mật mã khóa bí mật, mã PIN, OTP và không chia sẻ các thiết bị lưu trữ các thông tin này;

b) Nguyên tắc thiết lập mã khóa bí mật, mã PIN và thay đổi mã khóa bí mật, mã PIN của tài khoản giao dịch điện tử;

c) Không nên sử dụng máy tính công cộng để truy cập, thực hiện giao dịch; không nên sử dụng mạng WIFI công cộng khi sử dụng dịch vụ Online Banking;

d) Không lưu lại tên đăng nhập và mã khóa bí mật, mã PIN trên các trình duyệt;

đ) Thoát khỏi phần mềm ứng dụng Online Banking khi không sử dụng;

e) Nhận dạng và hành động xử lý một số tình huống lừa đảo, giả mạo trang tin điện tử, phần mềm ứng dụng Online Banking;

g) Cài đặt đầy đủ các bản vá lỗ hổng bảo mật của hệ điều hành, phần mềm ứng dụng Mobile Banking; xem xét cài đặt phần mềm phòng chống mã độc và cập nhật mẫu nhận diện mã độc mới nhất trên thiết bị cá nhân sử dụng để giao dịch;

h) Lựa chọn các hình thức xác nhận giao dịch có mức độ an toàn, bảo mật theo quy định và phù hợp với nhu cầu của khách hàng về hạn mức giao dịch;

i) Cảnh báo các rủi ro liên quan đến việc sử dụng dịch vụ Online Banking;

k) Không sử dụng các thiết bị di động đã bị phá khóa để tải và sử dụng phần mềm ứng dụng Online Banking, phần mềm tạo OTP;

l) Không cài đặt các phần mềm lạ, phần mềm không có bản quyền, phần mềm không rõ nguồn gốc;

m) Thông báo kịp thời cho đơn vị khi phát hiện các giao dịch bất thường;

n) Thông báo ngay cho đơn vị các trường hợp: mất, thất lạc, hư hỏng thiết bị tạo OTP, số điện thoại nhận tin nhắn SMS, thiết bị lưu trữ khóa bảo mật tạo chữ ký điện tử; bị lừa đảo hoặc nghi ngờ bị lừa đảo; bị tin tặc hoặc nghi ngờ bị tin tặc tấn công.

3. Đơn vị phải cung cấp cho khách hàng thông tin về đầu mối tiếp nhận thông tin, số điện thoại đường dây nóng và chỉ dẫn cho khách hàng quy trình, cách thức phối hợp xử lý các lỗi và sự cố trong quá trình sử dụng dịch vụ Online Banking.

4. Đơn vị phải giải thích cho khách hàng về những trường hợp cụ thể đơn vị sẽ liên lạc với khách hàng, cách thức, phương tiện liên lạc trong quá trình khách hàng sử dụng dịch vụ Online Banking.

Điều 19. Bảo mật thông tin khách hàng

Đơn vị phải áp dụng các biện pháp bảo đảm an toàn, bảo mật dữ liệu khách hàng, tối thiểu bao gồm:

1. Dữ liệu của khách hàng phải được bảo đảm an toàn, bảo mật theo quy định của pháp luật.

2. Thông tin sử dụng để xác nhận giao dịch của khách hàng bao gồm mã khóa bí mật, mã PIN, thông tin sinh trắc học khi lưu trữ phải áp dụng các biện pháp mã hóa hoặc che dấu để bảo đảm tính bí mật.

3. Thiết lập quyền truy cập đúng chức năng, nhiệm vụ cho nhân sự thực hiện nhiệm vụ truy cập dữ liệu khách hàng; có biện pháp giám sát mỗi lần truy cập.

4. Có biện pháp quản lý truy cập, tiếp cận các thiết bị, phương tiện lưu trữ dữ liệu của khách hàng để phòng chống nguy cơ lộ, lọt dữ liệu.

5. Thông báo cho khách hàng khi xảy ra sự cố làm lộ, lọt dữ liệu của khách hàng và báo cáo kịp thời về Ngân hàng Nhà nước Việt Nam (Cục Công nghệ thông tin).

Chương III

ĐIỀU KHOẢN THI HÀNH

Điều 20. Chế độ báo cáo

Các đơn vị cung cấp dịch vụ Online Banking có trách nhiệm gửi báo cáo bằng văn bản về Ngân hàng Nhà nước Việt Nam (Cục Công nghệ thông tin) như sau:

1. Báo cáo cung cấp dịch vụ Online Banking:

a) Thời hạn gửi báo cáo: Tối thiểu 10 ngày làm việc trước khi cung cấp chính thức dịch vụ Online Banking;

b) Nội dung báo cáo:

(i) Địa chỉ trang tin điện tử hoặc kho ứng dụng cung cấp dịch vụ;

(ii) Ngày cung cấp chính thức;

(iii) Các giải pháp kiểm tra khách hàng truy cập dịch vụ Online Banking; các hình thức xác nhận giao dịch áp dụng cho từng loại giao dịch và hạn mức giao dịch (nếu có);

(iv) Các bản sao chứng nhận về bảo đảm an toàn bảo mật, phòng, chống gian lận, giả mạo quy định tại khoản 5, khoản 7 Điều 11 Thông tư này.

2. Báo cáo đột xuất theo yêu cầu của Ngân hàng Nhà nước.

Điều 21. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước

1. Cục Công nghệ thông tin có trách nhiệm theo dõi, kiểm tra và phối hợp với các đơn vị liên quan để xử lý những vướng mắc phát sinh trong quá trình thực hiện Thông tư này.

2. Cơ quan Thanh tra, giám sát ngân hàng có trách nhiệm thanh tra, giám sát việc thi hành Thông tư này và xử lý các trường hợp vi phạm theo quy định của pháp luật.

3. Ngân hàng Nhà nước chi nhánh tỉnh, thành phố có trách nhiệm thanh tra, giám sát việc thực hiện Thông tư này tại các tổ chức cung ứng dịch vụ trung gian thanh toán trên địa bàn (trừ Công ty Cổ phần Thanh toán Quốc gia Việt Nam) và xử lý các trường hợp vi phạm theo quy định của pháp luật.

Điều 22. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 01 năm 2025, trừ trường hợp quy định tại khoản 2, khoản 3, khoản 4 Điều này.

2. Điểm b khoản 1 Điều 4, điểm d khoản 9 Điều 7, khoản 3 và khoản 4 Điều 8 có hiệu lực thi hành kể từ ngày 01 tháng 07 năm 2025.

3. Điểm b khoản 1 Điều 10 có hiệu lực thi hành kể từ ngày 01 tháng 01 năm 2026.

4. Điểm c khoản 5 Điều 11, điểm c khoản 7 Điều 11, điểm b (iv) khoản 1 Điều 20 có hiệu lực thi hành kể từ ngày 01 tháng 07 năm 2026.

5. Các văn bản sau đây hết hiệu lực kể từ ngày Thông tư này có hiệu lực:

a) Thông tư số 35/2016/TT-NHNN ngày 29 tháng 12 năm 2016 của Thống đốc Ngân hàng Nhà nước Việt Nam quy định về an toàn, bảo mật cho việc cung

cấp dịch vụ ngân hàng trên Internet;

b) Thông tư số 35/2018/TT-NHNN ngày 24 tháng 12 năm 2018 của Thống đốc Ngân hàng Nhà nước Việt Nam sửa đổi, bổ sung một số điều của Thông tư số 35/2016/TT-NHNN ngày 29 tháng 12 năm 2016 của Thống đốc Ngân hàng Nhà nước Việt Nam quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet.

6. Bãi bỏ Điều 25 của Thông tư số 09/2020/TT-NHNN ngày 21 tháng 10 năm 2020 của Thống đốc Ngân hàng Nhà nước Việt Nam quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng.

Điều 23. Quy định chuyển tiếp

1. Các giao dịch đăng ký tự động trích Nợ tài khoản thanh toán, tự động trích Nợ ví điện tử, tự động thanh toán từ thẻ của khách hàng được thực hiện trước ngày Thông tư này có hiệu lực thi hành được tiếp tục thực hiện đến hết thời hạn của thỏa thuận đã giao kết; trường hợp thỏa thuận không xác định thời hạn thì được tiếp tục thực hiện đến hết ngày 31 tháng 12 năm 2026. Việc sửa đổi, bổ sung, gia hạn thỏa thuận phải tuân thủ theo quy định tại khoản 2 Điều 10 Thông tư này.

2. Các mã khóa bí mật, mã PIN đang được sử dụng trước ngày Thông tư này có hiệu lực thi hành thì được tiếp tục sử dụng cho đến khi khách hàng thay đổi hoặc đến hết thời gian hiệu lực của mã khóa bí mật, mã PIN. Kể từ ngày Thông tư này có hiệu lực, các mã khóa bí mật, mã PIN khi thay đổi phải tuân thủ quy định tại khoản 1, khoản 2 Điều 11 Thông tư này.

Điều 24. Tổ chức thực hiện

Chánh Văn phòng, Cục trưởng Cục Công nghệ thông tin và Thủ trưởng các đơn vị thuộc Ngân hàng Nhà nước Việt Nam, Chủ tịch Hội đồng quản trị, Chủ tịch Hội đồng thành viên, Tổng giám đốc (Giám đốc) các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, các tổ chức cung ứng dịch vụ trung gian thanh toán, công ty thông tin tín dụng chịu trách nhiệm tổ chức thực hiện Thông tư này./.

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Phạm Tiến Dũng

Nơi nhận:
- Như Điều 24;
- Ban Lãnh đạo NHNN;
- Văn phòng Chính phủ;
- Bộ Tư pháp (để kiểm tra);
- Công báo;
- Lưu VP, PC, CNTT.

PHỤ LỤC 01

PHÂN LOẠI GIAO DỊCH THANH TOÁN TRỰC TUYẾN

(kèm theo Thông tư số 50 /2024/TT-NHNN ngày 31 tháng 10 năm 2024 của Thống đốc Ngân hàng Nhà nước)

STT	Loại hình giao dịch	Giao dịch loại A	Giao dịch loại B	Giao dịch loại C	Giao dịch loại D
I	**Khách hàng cá nhân**				
1	Nhóm I.1: - Chuyển tiền giữa các tài khoản thanh toán, thẻ ghi nợ, thẻ trả trước định danh (sau đây gọi chung là thẻ) của một khách hàng trong một tổ chức cung ứng dịch vụ thanh toán. - Chuyển tiền giữa các ví điện tử của một khách hàng trong một tổ chức cung ứng dịch vụ trung gian thanh toán.	Tất cả các giao dịch.			
2	Nhóm I.2: - Các giao dịch thanh toán hàng hóa, dịch vụ hợp pháp được tổ chức cung ứng dịch vụ thanh toán, trung gian thanh toán cung cấp hoặc tại các đơn vị chấp nhận thanh toán do các tổ chức cung ứng dịch vụ thanh toán, trung gian	Giao dịch thỏa mãn điều kiện: G + T ≤ 5 triệu VND.	Giao dịch thỏa mãn các điều kiện: (i) G + T > 5 triệu VND. (ii) G + T ≤ 100 triệu VND.	Giao dịch thỏa mãn các điều kiện: (i) G + T > 100 triệu VND. (ii) G + T ≤ 1,5 tỷ VND.	Giao dịch thỏa mãn điều kiện: G + T > 1,5 tỷ VND.

STT	Loại hình giao dịch	Giao dịch loại A	Giao dịch loại B	Giao dịch loại C	Giao dịch loại D
	thanh toán chịu trách nhiệm lựa chọn, thẩm định, giám sát và quản lý.				
3	Nhóm I.3: - Chuyển tiền giữa các tài khoản thanh toán, thẻ, ví điện tử của các chủ tài khoản, chủ thẻ, chủ ví điện tử khác nhau. - Chuyển tiền giữa các tài khoản, thẻ, ví điện tử mở tại các tổ chức cung ứng dịch vụ thanh toán, tổ chức phát hành thẻ, tổ chức cung ứng dịch vụ trung gian thanh toán khác nhau. - Nạp tiền vào Ví điện tử[1]. - Rút tiền ra khỏi Ví điện tử.	Giao dịch nạp, rút tiền giữa Ví điện tử và tài khoản đồng Việt Nam của chủ ví điện tử tại ngân hàng liên kết theo quy định của pháp luật thỏa mãn các điều kiện: (i) $G \leq 10$ triệu VND. (ii) $G + T_{ksth} \leq 20$ triệu VND.	Giao dịch (ngoại trừ giao dịch nạp, rút tiền giữa Ví điện tử và tài khoản đồng Việt Nam của chủ ví điện tử tại ngân hàng liên kết theo quy định của pháp luật) thỏa mãn các điều kiện: (i) $G \leq 10$ triệu VND. (ii) $G + T_{ksth} \leq 20$ triệu VND.	Giao dịch thỏa mãn một trong các trường hợp sau: 1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện: (i) $G \leq 10$ triệu VND. (ii) $G + T_{ksth} > 20$ triệu VND. (iii) $G + T \leq 1,5$ tỷ VND. 2. Trường hợp 2: Giao dịch thỏa mãn các điều kiện: (i) $G > 10$ triệu VND. (ii) $G \leq 500$ triệu VND. (iii) $G + T \leq 1,5$ tỷ VND.	Giao dịch thỏa mãn một trong các trường hợp sau: 1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện: (i) $G \leq 10$ triệu VND. (ii) $G + T_{ksth} > 20$ triệu VND. (iii) $G + T > 1,5$ tỷ VND. 2. Trường hợp 2: Giao dịch thỏa mãn các điều kiện: (i) $G > 10$ triệu VND. (ii) $G \leq 500$ triệu VND. (iii) $G + T > 1,5$ tỷ VND. 3. Trường hợp 3: Giao dịch thỏa mãn điều kiện: $G > 500$ triệu VND.

STT	Loại hình giao dịch	Giao dịch loại A	Giao dịch loại B	Giao dịch loại C	Giao dịch loại D
4	Nhóm I.4: Chuyển tiền liên ngân hàng ra nước ngoài[2].			Giao dịch thỏa mãn các điều kiện: (i) G ≤ 200 triệu VND. (ii) G + T ≤ 1 tỷ VND.	Giao dịch thỏa mãn một trong các trường hợp sau: 1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện: (i) G ≤ 200 triệu VND. (ii) G + T > 1 tỷ VND. 2. Trường hợp 2: Giao dịch thỏa mãn điều kiện: G > 200 triệu VND.
II	**Khách hàng tổ chức[3]**				
1	Nhóm II.1: Chuyển tiền giữa các tài khoản thanh toán hoặc Ví điện tử của cùng một khách hàng trong một tổ chức cung ứng dịch vụ thanh toán hoặc tổ chức cung ứng dịch vụ trung gian thanh toán.		Tất cả các giao dịch.		
2	Nhóm II.2: - Chuyển tiền giữa các tài khoản thanh toán, ví điện tử của các chủ tài khoản, chủ ví điện tử khác nhau. - Chuyển tiền giữa các tài khoản, ví điện tử mở tại các tổ chức cung ứng dịch			Giao dịch thỏa mãn các điều kiện: (i) G ≤ 1 tỷ VND. (ii) G + T ≤ 10 tỷ VND.	Giao dịch thỏa mãn một trong các trường hợp sau: 1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện: (i) G ≤ 1 tỷ VND. (ii) G + T > 10 tỷ VND.

STT	Loại hình giao dịch	Giao dịch loại A	Giao dịch loại B	Giao dịch loại C	Giao dịch loại D
	vụ thanh toán, tổ chức cung ứng dịch vụ trung gian thanh toán khác nhau. - Các giao dịch thanh toán hàng hóa, dịch vụ hợp pháp được tổ chức cung ứng dịch vụ thanh toán, trung gian thanh toán cung cấp hoặc tại các đơn vị chấp nhận thanh toán do các tổ chức cung ứng dịch vụ thanh toán, trung gian thanh toán chịu trách nhiệm lựa chọn, thẩm định, giám sát và quản lý. - Nạp tiền vào Ví điện tử[1]. - Rút tiền ra khỏi Ví điện tử.				2. Trường hợp 2: Giao dịch thỏa mãn điều kiện: G > 1 tỷ VND.
3	Nhóm II.3: Chuyển tiền liên ngân hàng ra nước ngoài[2].			Giao dịch thỏa mãn các điều kiện: (i) G ≤ 500 triệu VND. (ii) G + T ≤ 5 tỷ VND.	Giao dịch thỏa mãn một trong các trường hợp sau: 1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện: (i) G ≤ 500 triệu VND. (ii) G + T > 5 tỷ VND. 2. Trường hợp 2: Giao dịch thỏa mãn điều kiện: G > 500 triệu VND.

Ghi chú:

G: Giá trị của giao dịch.

$T_{ksth:}$ Tổng giá trị các giao dịch loại A và loại B của từng nhóm loại hình giao dịch đã thực hiện của một tài khoản thanh toán hoặc một thẻ (*bao gồm cả giao dịch nạp tiền vào ví điện tử*) hoặc một ví điện tử (*không bao gồm giao dịch nạp tiền vào ví điện tử*) của khách hàng tại một tổ chức cung ứng dịch vụ thanh toán hoặc tổ chức cung ứng dịch vụ trung gian thanh toán, không bao gồm các giao dịch chủ động trích Nợ tài khoản thanh toán, chủ động trích Nợ ví điện tử, chủ động thanh toán từ thẻ. T_{ksth} được tính giá trị bằng 0 tại thời điểm đầu ngày hoặc ngay sau khi khách hàng có phát sinh giao dịch trong ngày sử dụng hình thức xác nhận cho giao dịch loại C hoặc loại D.

T: Tổng giá trị các giao dịch của từng nhóm loại hình giao dịch đã thực hiện trong ngày (*của một tài khoản thanh toán hoặc một thẻ (bao gồm cả giao dịch nạp tiền vào ví điện tử) hoặc một ví điện tử (không bao gồm giao dịch nạp tiền vào ví điện tử)* của khách hàng tại một tổ chức cung ứng dịch vụ thanh toán hoặc tổ chức cung ứng dịch vụ trung gian thanh toán), không bao gồm các giao dịch chủ động trích Nợ tài khoản thanh toán, chủ động trích Nợ ví điện tử, chủ động thanh toán từ thẻ.

(1) Đối với giao dịch nạp tiền vào Ví điện tử từ tài khoản đồng Việt Nam của chủ ví điện tử tại ngân hàng liên kết, việc phân loại giao dịch căn cứ theo tài khoản thanh toán liên kết với Ví điện tử.

(2) Hạn mức quy đổi theo tỷ giá tại thời điểm thực hiện giao dịch.

(3) Trường hợp khách hàng là hộ kinh doanh hoặc doanh nghiệp siêu nhỏ áp dụng chế độ kế toán đơn giản, việc phân loại giao dịch tương tự khách hàng cá nhân.

PHỤ LỤC 02
XÁC NHẬN GIAO DỊCH THANH TOÁN TRỰC TUYẾN

(ban hành kèm theo Thông tư số 50 /2024/TT-NHNN ngày 31 tháng 10 năm 2024 của Thống đốc Ngân hàng Nhà nước)

STT	Giao dịch	Hình thức xác nhận giao dịch thanh toán trực tuyến tối thiểu	
		Khách hàng cá nhân	**Khách hàng tổ chức**
1	Giao dịch loại A	- Mã khóa bí mật hoặc mã PIN (trường hợp đã xác nhận tại bước đăng nhập thì không bắt buộc phải xác nhận tại bước thực hiện giao dịch).	- Mã khóa bí mật hoặc mã PIN (trường hợp đã xác nhận tại bước đăng nhập thì không bắt buộc phải xác nhận tại bước thực hiện giao dịch).
2	Giao dịch loại B	- SMS OTP hoặc Voice OTP hoặc Email OTP; - Hoặc Thẻ ma trận OTP; - Hoặc Soft OTP/ Token OTP loại cơ bản hoặc nâng cao; - Hoặc hai kênh; - Hoặc khớp đúng thông tin sinh trắc học thiết bị[1]; - Hoặc FIDO; - Hoặc chữ ký điện tử; - Hoặc chữ ký điện tử an toàn.	- SMS OTP hoặc Voice OTP hoặc Email OTP; - Hoặc Thẻ ma trận OTP; - Hoặc khớp đúng thông tin sinh trắc học thiết bị của người đại diện hợp pháp hoặc cá nhân được người đại diện hợp pháp ủy quyền (nếu có).
3	Giao dịch loại C	- OTP gửi qua SMS/Voice hoặc Soft OTP/Token OTP loại cơ bản hoặc chữ ký điện tử, - Và kết hợp khớp đúng thông tin sinh trắc học.	- Soft OTP/Token OTP loại cơ bản; - Hoặc hai kênh; - Hoặc chữ ký điện tử.
4	Giao dịch loại D	- Soft OTP/Token OTP loại nâng cao hoặc FIDO hoặc chữ ký điện tử an toàn, - Và kết hợp khớp đúng thông tin sinh trắc học.	- Soft OTP/Token OTP loại nâng cao; - Hoặc FIDO; - Hoặc chữ ký điện tử an toàn.

Ghi chú:

- Các hình thức xác nhận quy định chi tiết tại Điều 11 Thông tư này.
- Hình thức xác nhận giao dịch loại D có thể xác nhận giao dịch loại A, B, C.
- Hình thức xác nhận giao dịch loại C có thể xác nhận giao dịch loại A, B.
- Hình thức xác nhận giao dịch loại B có thể xác nhận giao dịch loại A.
- Trường hợp khách hàng là hộ kinh doanh hoặc doanh nghiệp siêu nhỏ áp dụng chế độ kế toán đơn giản, áp dụng hình thức xác nhận giao dịch tương tự khách hàng cá nhân. Trong đó, đối với hình thức khớp đúng thông tin sinh trắc học và hình thức khớp đúng thông tin sinh trắc học thiết bị, thông tin sinh trắc học sử dụng để đối chiếu, so sánh là của người đại diện hợp pháp hoặc cá nhân được người đại diện hợp pháp ủy quyền (nếu có).

(1) Trường hợp khách hàng đã đăng nhập ứng dụng Online Banking bằng khớp đúng thông tin sinh trắc học thiết bị, không áp dụng biện pháp xác nhận này khi thực hiện giao dịch trong phiên đăng nhập đó.

PHỤ LỤC 03

PHÂN LOẠI GIAO DỊCH THANH TOÁN THẺ TRỰC TUYẾN

(ban hành kèm theo Thông tư số 50 /2024/TT-NHNN ngày 31 tháng 10 năm 2024 của Thống đốc Ngân hàng Nhà nước)

STT	Loại hình giao dịch	Giao dịch loại E	Giao dịch loại F	Giao dịch loại G
1	Các giao dịch thanh toán hàng hóa, dịch vụ hợp pháp được tổ chức cung ứng dịch vụ thanh toán cung cấp hoặc tại các đơn vị chấp nhận thẻ do các tổ chức cung ứng dịch vụ thanh toán chịu trách nhiệm lựa chọn, thẩm định, giám sát và quản lý.	Giao dịch thỏa mãn điều kiện: G + T ≤ 5 triệu VND.	Giao dịch thỏa mãn các điều kiện: (i) G + T > 5 triệu VND. (ii) G + T ≤ 100 triệu VND.	Giao dịch thỏa mãn các điều kiện: G + T > 100 triệu VND.

Ghi chú:

G: Giá trị của giao dịch.

T: Tổng giá trị các giao dịch đã thực hiện trong ngày của thẻ đang giao dịch của khách hàng tại một tổ chức phát hành thẻ, không bao gồm các giao dịch do tổ chức phát hành thẻ chủ động thanh toán từ thẻ theo thỏa thuận với khách hàng.

PHỤ LỤC 04
XÁC NHẬN GIAO DỊCH THANH TOÁN THẺ TRỰC TUYẾN

(ban hành kèm theo Thông tư số 50 /2024/TT-NHNN ngày 31 tháng 10 năm 2024 của Thống đốc Ngân hàng Nhà nước)

STT	Giao dịch	Hình thức xác nhận giao dịch thanh toán thẻ trực tuyến tối thiểu
1	Giao dịch loại E	Mã khóa bí mật hoặc mã PIN (trường hợp đã xác nhận tại bước đăng nhập thì không bắt buộc phải xác nhận tại bước thực hiện giao dịch).
2	Giao dịch loại F	- SMS OTP hoặc Voice OTP hoặc Email OTP; - Hoặc Thẻ ma trận OTP; - Hoặc Soft OTP/ Token OTP loại cơ bản; - Hoặc khớp đúng thông tin sinh trắc học thiết bị; - Hoặc hai kênh.
3	Giao dịch loại G	- Soft OTP/Token OTP loại nâng cao; - Hoặc FIDO; - Hoặc chữ ký điện tử/ chữ ký điện tử an toàn; - Hoặc EMV 3DS.

Ghi chú:

- Các hình thức xác nhận quy định chi tiết tại Điều 11 Thông tư này.
- Hình thức xác nhận giao dịch loại G có thể xác nhận giao dịch loại E, F.
- Hình thức xác nhận giao dịch loại F có thể xác nhận giao dịch loại E.