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.