NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 630 /QĐ-NHNN	*Hà Nội, ngày 31 tháng 3 năm 2017*

QUYẾT ĐỊNH
Ban hành Kế hoạch áp dụng các giải pháp về an toàn bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng

THỐNG ĐỐC NGÂN HÀNG NHÀ NƯỚC

Căn cứ Luật Ngân hàng Nhà nước Việt Nam số 46/2010/QH12 ngày 16 tháng 6 năm 2010;

Căn cứ Nghị định số 16/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;

Căn cứ Thông tư số 35/2016/TT-NHNN ngày 29 tháng 12 năm 2016 của Ngân hàng Nhà nước quy định an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet;

Xét đề nghị của Cục trưởng Cục Công nghệ thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Kế hoạch áp dụng giải pháp về an toàn bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký ban hành.

Điều 3. Chánh Văn phòng, Cục trưởng Cục Công nghệ thông tin và Thủ trưởng các đơn vị thuộc Ngân hàng Nhà nước Việt Nam, Giám đốc Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc Trung ương; 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 chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Ban Lãnh đạo NHNN;
- Lưu: VP, CNTH.

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Nguyễn Kim Anh

NGÂN HÀNG NHÀ NƯỚC
VIỆT NAM

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

KẾ HOẠCH
Áp dụng các giải pháp về an toàn bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngành Ngân hàng

(Ban hành kèm theo Quyết định số 630 /QĐ-NHNN ngày 31 tháng 3 năm 2017 của Thống đốc Ngân hàng Nhà nước)

A. MỤC TIÊU

- Tăng cường vai trò quản lý nhà nước của Ngân hàng Nhà nước đối với công tác an ninh CNTT và dịch vụ, tiện ích thanh toán trực tuyến, thanh toán thẻ.

- Nâng cao chất lượng quản lý rủi ro CNTT và tăng cường an ninh bảo mật các dịch vụ ngân hàng trực tuyến và thanh toán thẻ của các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài và tổ chức cung ứng dịch vụ trung gian thanh toán.

B. NHIỆM VỤ VÀ LỘ TRÌNH

I. Đối với các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán

1. Triển khai áp dụng các giải pháp công nghệ xác thực mới trong thanh toán trực tuyến trên Internet (Internet Banking, Mobile Banking)

Căn cứ phân loại giao dịch theo hạn mức tại Phụ lục 01 đính kèm, từ **01/01/2019** các tổ chức cung ứng dịch vụ thanh toán, trung gian thanh toán trên mạng Internet phải triển khai áp dụng các giải pháp xác thực tối thiểu như sau:

STT	Giao dịch[1]	Biện pháp xác thực tối thiểu[2]
1	Giao dịch loại A	- Tên đăng nhập, mật khẩu hoặc mã PIN
2	Giao dịch loại B	- SMS OTP. - Hoặc Thẻ ma trận OTP. - Hoặc Token OTP loại cơ bản, không có chức năng xác thực người dùng sử dụng Token.
3	Giao dịch loại C	- Soft OTP hoặc Token OTP loại cơ bản, có chức năng xác thực người dùng sử dụng phần mềm, Token. - Giải pháp xác thực qua hai kênh. - Hoặc xác thực bằng dấu hiệu nhận dạng sinh trắc học.

[1] Phân loại giao dịch tham khảo tại Phụ lục 01.
[2] Chi tiết về các giải pháp xác thực tham khảo tại Phụ lục 02.

4	Giao dịch loại D	- Soft OTP hoặc Token OTP loại nâng cao, có chức năng ký giao dịch. - Hoặc xác thực bằng thiết bị U2F/UAF. - Hoặc xác thực bằng chứng thư số.

Ghi chú:

- Biện pháp xác thực giao dịch loại D có thể xác thực giao dịch loại A, B, C.
- Biện pháp xác thực giao dịch loại C có thể xác thực giao dịch loại A, B.
- Biện pháp xác thực giao dịch loại B có thể xác thực giao dịch loại A.
- Trường hợp các đơn vị sử dụng các biện pháp xác thực khác các loại trên thì báo cáo Ngân hàng Nhà nước (qua Cục Công nghệ thông tin) trước khi áp dụng.

2. Triển khai áp dụng các giải pháp giảm thiểu rủi ro trong thanh toán thẻ

Các tổ chức cung ứng dịch vụ thanh toán thẻ phải triển khai các giải pháp giảm thiểu rủi ro theo lộ trình như sau:

STT	Giải pháp	Thời hạn hoàn thành
1	Thông báo giao dịch qua tin nhắn SMS hoặc thư điện tử	01/01/2018
2	Thiết lập hạn mức giao dịch trong ngày.	01/01/2019
3	Thiết lập tính năng cho phép/ không cho phép thanh toán trực tuyến.	01/01/2019
4	Thiết lập hạn mức thanh toán thẻ trực tuyến trong ngày.	01/01/2019
5	Thiết lập tính năng cho phép/ không cho phép thanh toán ở nước ngoài (ngoại trừ các giao dịch trực tuyến)	01/01/2019
6	Triển khai giải pháp xác thực 3D Secure (hoặc tương đương) cho việc thanh toán trực tuyến với thẻ quốc tế.	01/01/2019

3. Trong quá trình triển khai, nếu có khó khăn, vướng mắc, các đơn vị báo cáo về Ngân hàng Nhà nước (qua Cục Công nghệ thông tin) để phối hợp xử lý.

II. Đối với các đơn vị Ngân hàng Nhà nước

1. Vụ Truyền thông phối hợp với các đơn vị liên quan thực hiện công tác truyền thông đến người dân, doanh nghiệp hỗ trợ hiệu quả cho việc áp dụng các tiêu chuẩn, các giải pháp xác thực trong thanh toán trực tuyến và thanh toán thẻ.

2. Vụ Thanh toán có trách nhiệm phối hợp với Cục Công nghệ thông tin theo dõi, giám sát và kiểm tra việc triển khai Kế hoạch này.

3. Cục Công nghệ thông tin có trách nhiệm theo dõi, đôn đốc thực hiện việc áp dụng. Định kỳ hằng năm hoặc đột xuất (khi cần thiết) tổng hợp tình hình, báo cáo Thống đốc NHNN.

Nơi nhận:
- Ban Lãnh đạo NHNN;
- Các đơn vị, Vụ, Cục thuộc NHNN.
- Các TCTD, chi nhánh ngân hàng nước ngoài;
- Các tổ chức cung ứng dịch vụ trung gian thanh toán;
- Lưu Văn phòng, Cục CNTT.

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Nguyễn Kim Anh

PHỤ LỤC 01: PHÂN LOẠI GIAO DỊCH

STT	Loại giao dịch	Giao dịch loại A	Giao dịch loại B	Giao dịch loại C	Giao dịch loại D
I	**Khách hàng cá nhân**				
1	- Các giao dịch tra cứu thông tin - Chuyển tiền trong ngân hàng, cùng chủ tài khoản	Tất cả các giao dịch			
2	Các giao dịch thanh toán hoá đơn dịch vụ với mã khách hàng cố định (như dịch vụ điện, nước, viễn thông, phí giao thông).	Giao dịch có hạn mức: + Hạn mức giao dịch 1 ngày ≤ 5 triệu VND	Giao dịch có hạn mức: + Hạn mức giao dịch 1 ngày > 5 triệu VND đến 100 triệu VND và theo đăng ký của khách hàng.		
3	Chuyển tiền trong ngân hàng, khác chủ tài khoản		Giao dịch có hạn mức: + Hạn mức giao dịch 1 ngày ≤ 100 triệu VND	Giao dịch có hạn mức: + Hạn mức 1 giao dịch < 500 triệu VND + Hạn mức giao dịch 1 ngày < 1,5 tỷ VND	Giao dịch có hạn mức: + Hạn mức 1 giao dịch ≥ 500 triệu VND + Hạn mức giao dịch 1 ngày theo đăng ký của khách hàng
4	Chuyển tiền liên ngân hàng trong nước		Giao dịch có hạn mức: + Hạn mức giao dịch 1 ngày ≤ 100 triệu VND	Giao dịch có hạn mức: + Hạn mức 1 giao dịch < 500 triệu VND + Hạn mức giao dịch 1 ngày < 1,5 tỷ VND	Giao dịch có hạn mức: + Hạn mức 1 giao dịch ≥ 500 triệu VND + Hạn mức giao dịch 1 ngày theo đăng ký của khách hàng
5	Chuyển tiền liên ngân hàng ra nước ngoài			Giao dịch có hạn mức: + Hạn mức 1 giao dịch < 200 triệu VND + Hạn mức giao dịch 1 ngày < 1 tỷ VND	Giao dịch có hạn mức: + Hạn mức 1 giao dịch ≥ 200 triệu VND + Hạn mức giao dịch 1 ngày theo đăng ký của khách hàng

II	**Khách hàng doanh nghiệp**				
1	Các giao dịch tra cứu thông tin	Tất cả các giao dịch			
2	Chuyển tiền trong ngân hàng, cùng chủ tài khoản		Tất cả các giao dịch		
3	Chuyển tiền trong ngân hàng, khác chủ tài khoản			Giao dịch có hạn mức: + Hạn mức 1 giao dịch < 1 tỷ VND + Hạn mức giao dịch 1 ngày < 10 tỷ VND	Giao dịch có hạn mức: + Hạn mức 1 giao dịch ≥ 1 tỷ VND + Hạn mức giao dịch 1 ngày theo đăng ký của khách hàng
4	Chuyển tiền liên ngân hàng trong nước			Giao dịch có hạn mức: + Hạn mức 1 giao dịch < 1 tỷ VND + Hạn mức giao dịch 1 ngày < 10 tỷ VND	Giao dịch có hạn mức: + Hạn mức 1 giao dịch ≥ 1 tỷ VND + Hạn mức giao dịch 1 ngày theo đăng ký của khách hàng
5	Chuyển tiền liên ngân hàng ra nước ngoài			Giao dịch có hạn mức: + Hạn mức 1 giao dịch < 500 triệu VND + Hạn mức giao dịch 1 ngày < 5 tỷ VND	Giao dịch có hạn mức: + Hạn mức 1 giao dịch ≥ 500 triệu VND + Hạn mức giao dịch 1 ngày theo đăng ký của khách hàng

PHỤ LỤC 02: CÁC GIẢI PHÁP XÁC THỰC GIAO DỊCH TRỰC TUYẾN

STT	Giải pháp	Chi tiết về giải pháp
1	**SMS OTP**	Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống ngân hàng trực tuyến sẽ gửi tin nhắn SMS có chứa mã OTP tới điện thoại khách hàng đã đăng ký trước. Khách hàng nhập mã OTP trên giao diện thanh toán trực tuyến để hoàn thành giao dịch để thanh toán.
2	**Thẻ ma trận OTP**	Thẻ ma trận là một bảng 2 chiều (dòng, cột), tương ứng với mỗi dòng, cột là một mã OTP. Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống ngân hàng trực tuyến sẽ thông báo số dòng, cột trên thẻ ma trận để khách hàng nhập mã OTP tương ứng hoàn thành giao dịch thanh toán.
3	**Soft OTP loại cơ bản**	Phần mềm tạo mã OTP (**Soft OTP**) thường được cài đặt trên điện thoại di động/ máy tính bảng đã đăng ký với Ngân hàng. Đối với loại cơ bản, mã OTP được sinh ngẫu nhiên theo thời gian, đồng bộ với hệ thống thanh toán trực tuyến tại ngân hàng. Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống ngân hàng trực tuyến yêu cầu khách hàng nhập mã OTP được sinh bởi Soft OTP để hoàn thành giao dịch thanh toán.
4	**Soft OTP loại nâng cao**	**Soft OTP** loại nâng cao thường được cài đặt trên điện thoại di động/ máy tính bảng đã đăng ký với Ngân hàng. Đối với loại nâng cao, mã OTP được tạo kết hợp với mã của từng giao dịch (transaction signing). Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống ngân hàng trực tuyến tạo ra một mã giao dịch thông báo cho khách hàng. Khách hàng nhập mã giao dịch vào Soft OTP để phần mềm tạo ra mã OTP. Sau đó khách hàng nhập mã OTP trên giao diện thanh toán trực tuyến để hoàn thành giao dịch thanh toán.
5	**Token OTP loại cơ bản**	Token OTP là thiết bị tạo mã OTP. Đối với loại cơ bản, mã OTP được sinh ngẫu nhiên theo thời gian, đồng bộ với hệ thống thanh toán trực tuyến tại ngân hàng. Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống ngân hàng trực tuyến yêu cầu khách hàng nhập mã OTP được sinh bởi Token OTP để hoàn thành giao dịch thanh toán.
6	**Token OTP loại nâng cao**	Token OTP loại nâng cao là thiết bị tạo mã OTP. Trong đó mã OTP được tạo kết hợp với mã của từng giao dịch (transaction signing). Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống ngân hàng trực tuyến 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. Sau đó khách hàng nhập mã OTP trên giao diện thanh toán trực tuyến để hoàn thành giao dịch thanh toán.
7	**Xác thực hai kênh**	Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống gửi thông tin yêu cầu xác thực giao dịch đến thiết bị di động của khách hàng qua kênh thoại hoặc qua mã USSD 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.
8	**Sinh trắc học**	Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống ngân hàng trực tuyến yêu cầu khách hàng trình diện dấu hiệu nhận dạng sinh trắc học của khách hàng khó có khả năng làm giả để xác thực giao dịch (như khuôn mặt, tĩnh mạch ngón tay hoặc bàn tay, mống mắt,

		giọng nói).
9	**Universal 2nd Factor/ Universal Authentication Framework (U2F/UAF)**	Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống ngân hàng trực tuyến yêu cầu khách hàng sử dụng thiết bị U2F/UAF giao tiếp qua cổng USB hoặc không dây (Bluetooth, NFC). Sau khi xác thực sử dụng thiết bị bằng mã truy cập hoặc dấu hiệu sinh trắc học, thiết bị U2F/UAF sẽ tự động giao tiếp với trình duyệt và máy chủ xác thực để xác thực địa chỉ website IB và giao dịch.
10	**Chữ ký số**	Khi thực hiện giao dịch thanh toán trực tuyến, hệ thống ngân hàng trực tuyến yêu cầu khách hàng nhập chứng thư số (lưu trên thiết bị USB hoặc SIM điện thoại) Khách hàng phải nhập mã truy cập thiết bị USB hoặc SIM điện thoại và chọn chứng thư số để ký giao dịch.