|  |  |
| --- | --- |
| NGÂN HÀNG NHÀ NƯỚC  VIỆT NAM  **CỤC CÔNG NGHỆ THÔNG TIN** | CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆTNAM  **Độc lập - Tự do - Hạnh phúc** Hà Nội, ngày tháng 06 năm 2024 |

**BẢN THUYẾT MINH DỰ THẢO**

**Thông tư thay thế Thông tư 35/2016/TT-NHNN**

1. **Sự cần thiết phải ban hành Thông tư thay thế Thông tư 35/2016/TT-NHNN**

Thông tư 35/2016/TT-NHNN ngày 29/12/2016 (sửa đổi, bổ sung tại Thông tư 35/2018/TT-NHNN ngày 24/12/2018) của Thống đốc Ngân hàng Nhà nước được ban hành đã tạo hành lang pháp lý và hướng dẫn các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức trung gian thanh toán trong công tác bảo đảm an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng, dịch vụ trung gian thanh toán trên Internet. Nhằm cập nhật đầy đủ các quy định của pháp luật về công tác bảo đảm an ninh, an toàn thông tin, giao dịch điện tử và xác thực điện tử, đồng thời phù hợp với thực tế tình hình an toàn thông tin mạng trong ngành Ngân hàng, Ngân hàng Nhà nước Việt Nam (Cục Công nghệ thông tin) đã nghiên cứu, hoàn thành Dự thảo Thông tư thay thế Thông tư 35/2016/TT-NHNN (sau đây gọi là Dự thảo Thông tư).

1. ***Cơ sở pháp lý***

Trong những năm gần đây, Quốc hội, Chính phủ đã ban hành một số văn bản pháp luật có điều chỉnh đến công tác bảo đảm an ninh, an toàn thông tin, giao dịch điện tử và xác thực điện tử trong ngành Ngân hàng:

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

- Luật Căn cước ngày 27 tháng 11 năm 2023;

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

- Nghị định số 59/2022/NĐ-CP ngày 05/9/2022 quy định về định danh và xác thực điện tử;

- Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân.

Triển khai Quyết định số 2521/QĐ-NHNN ngày 29/12/2023 của Thống đốc NHNN về việc Ban hành Chương trình xây dựng Thông tư năm 2024 của NHNN.

1. ***Cơ sở thực tiễn***

Tình hình an ninh mạng tại Việt Nam hiện nay diễn ra phức tạp, ngành Ngân hàng, tài chính là một trong các ngành thuộc đích nhắm hàng đầu của tội phạm sử dụng công nghệ cao. Tội phạm sử dụng không gian mạng để lừa đảo chiếm đoạt tài sản gia tăng, các đối tượng sử dụng tài khoản ngân hàng, ví điện tử không chính chủ để nhận, chuyển tiền lừa đảo, sau đó thông qua tiền ảo (USDT, Bitcoin,…) để làm công cụ rửa tiền gây thiệt hại về tài sản của khách hàng và ngân hàng. Ngày 18/12/2023, NHNN đã ban hành Quyết định 2345/QĐ-NHNN về việc triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng. Theo đó từ 1/7/2024 các TCTD, trung gian thanh toán phải triển khai xác thực sinh trắc học bằng khuôn mặt từ nguồn dữ liệu dân cư (thông qua CCCD gắn chíp, VNeID) khi khách hàng cá nhân thực hiện các giao dịch trực tuyến có giá trị > 10 triệu đồng hoặc khi tổng giao dịch/ngày > 20 triệu đồng. Việc triển khai quyết định này sẽ nâng cao an toàn, bảo mật cho các giao dịch thanh toán trực tuyến, giảm thiểu rủi ro gian lận, lừa đảo trong giao dịch thanh toán trực tuyến. Để các quy định tại Quyết định 2345 có giá trị pháp lý cao hơn thì các quy định này sẽ được đưa vào trong Thông tư của Thống đốc NHNN.

Ngoài ra, hiện nay, nhiều tổ chức tín dụng, trung gian thanh toán đã triển khai giải pháp định danh, xác minh khách hàng trực tuyến (eKYC) bằng dấu hiệu sinh trắc học. Tuy nhiên tại Việt Nam chưa có tiêu chuẩn kỹ thuật quy định về nội dung này. Cục CNTT đã khảo sát tình hình triển khai xác thực sinh trắc học tại các đơn vị trong ngành và tham khảo các tiêu chuẩn quốc tế và đề xuất bổ sung quy định về tiêu chuẩn xác thực bằng dấu hiệu nhận dạng sinh trắc học tại Dự thảo Thông tư.

Bên cạnh đó, qua công tác kiểm tra và khảo sát, Cục CNTT đã ghi nhận được các khó khăn, vướng mắc và các đề xuất trong quá trình triển khai thực hiện Thông tư 35/2016/TT-NHNN tại các tổ chức tín dụng, tổ chức cung ứng dịch vụ trung gian thanh toán. Dự thảo Thông tư thay thế sẽ cập nhật, bổ sung một số nội dung giải quyết các khó khăn vướng mắc trong hoạt động cung cấp dịch vụ trực tuyến tại các tổ chức trong ngành Ngân hàng.

1. **Nguyên tắc, định hướng xây dựng Dự thảo Thông tư**

* Về bảo đảm an toàn hệ thống thông tin trong hoạt động ngân hàng (bao gồm an toàn hệ thống thông tin cung cấp dịch vụ trực tuyến – Online Banking), Thống đốc NHNN đã ban hành Thông tư 09/2020/TT-NHNN ngày 21/10/2020. Dự thảo Thông tư được xây dựng theo nguyên tắc:

+ Quy định rõ nguyên tắc Hệ thống Online Banking phải tuân thủ theo 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 và quy định của NHNN về an toàn hệ thống thông tin trong hoạt động ngân hàng.

+ Bổ sung các nội dung quy định đặc thù hoặc tăng cường an toàn, bảo mật cho hệ thống Online Banking, cụ thể như việc bảo đảm an toàn cho phần mềm ứng dụng, xác thực giao dịch điện tử, bảo vệ quyền lợi của khách hàng.

* Triển khai các văn bản pháp luật mới ban hành (nêu tại Mục I.1), Dự thảo Thông tin được bổ sung các quy định, hướng dẫn thực hiện trong ngành Ngân hàng.

Các quy định được sửa đổi, bổ sung, loại bỏ được nêu chi tiết trong Phụ lục 01 – Bảng so sánh Thông tư 35/2016/TT-NHNN và Dự thảo Thông tư (đính kèm).

1. **Kết cấu của Thông tư**

Dự thảo Thông tư gồm 03 Chương 24 Điều và 02 Phụ lục, cụ thể:

* ***Chương I. Quy định chung***

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

+ Điều 2. Giải thích từ ngữ và thuật ngữ

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

* ***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 ninh bảo mật

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

+ Điều 6. Hệ quản trị cơ sở dữ liệu

+ Điều 7. Phần mềm ứng dụng Online Banking

+ Điều 8. Phần mềm ứng dụng Mobile Banking

Mục 2. Xác thực giao dịch Online Banking

+ Điều 9. Xác thực khách hàng truy cập dịch vụ Online Banking

+ Điều 10. Xác thực giao dịch điện tử

+ Điều 11. Các hình thức xác thực giao dịch điện tử

Mục 3. Quản lý vận hành

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

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

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

+ Điều 15. Hệ thống quản trị, giám sát hoạt động của hệ thống Online Banking

+ Điều 16. Đảm bảo hoạt động liên tục

Mục 4. Bảo vệ quyền lợi của khách hàng

+ Điều 17. Thông tin về dịch vụ Online Banking

+ Điều 18. Bảo đảm an toàn cho khách hàng trong giao dịch thanh toán thẻ trực tuyến

+ Điều 19. Hướng dẫn khách hàng sử dụng dịch vụ Online Banking

+ Điều 20. Bảo mật thông tin khách hàng

* ***Chương III. Điều khoản thi hành***

+ Điều 21. Chế độ báo cáo

+ Điều 22. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước

+ Điều 23. Hiệu lực thi hành

+ Điều 24. Tổ chức thực hiện

- ***Phụ lục 01. Phân loại giao dịch theo các nhóm loại hình giao dịch trong thanh toán trực tuyến.***

***- Phụ lục 02. Các hình thức xác thực giao dịch điện tử trong thanh toán trực tuyến.***

1. **Các nội dung chính cần lấy ý kiến**
2. Bổ sung phạm vi, đối tượng áp dụng
3. Về phạm vi

Dự thảo Thông tư đã mở rộng phạm vi quy định về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng (Online Banking), không chỉ là các dịch vụ ngân hàng, dịch vụ trung gian thanh toán trên Internet (Internet Banking), mà mở rộng bao gồm các dịch vụ khác được Thống đốc NHNN chấp thuận hoặc quy định như dịch vụ thông tin tín dụng, dịch vụ ngoại hối, dịch vụ lưu ký chứng khoán, dịch vụ liên quan đến bao thanh toán, thư tín dụng,… quy định tại Luật Các tổ chức tín dụng năm 2024.

1. Về đối tượng

Dự thảo Thông tư bổ sung đối tượng công ty thông tin tín dụng là đối tượng cung cấp dịch vụ thông tin tín dụng.

1. Bổ sung quy định về các hình thức xác thực điện tử mà không phải là chữ ký điện tử theo Luật Giao dịch điện tử năm 2023

Căn cứ pháp lý: khoản 4 Điều 22 Luật Giao dịch điện tử năm 2023 “*Việc sử dụng các hình thức xác nhận khác bằng phương tiện điện tử để thể hiện sự chấp thuận của chủ thể ký đối với thông điệp dữ liệu mà không phải là chữ ký điện tử thực hiện theo quy định khác của pháp luật có liên quan*”.

Hiện nay, các hoạt động ngân hàng giao dịch bằng phương thức điện tử (thanh toán, cho vay,…), các ngân hàng thường sử dụng các giải pháp như mã PIN, OTP, sinh trắc học,… được NHNN quy định tại Quyết định 630/QĐ-NHNN[[1]](#footnote-1) (được thay thế bằng Quyết định 2345/QĐ-NHNN[[2]](#footnote-2) có hiệu lực từ 01/7/2024) để xác nhận sự chấp thuận của khách hàng. Đây là những hình thức xác nhận sự chấp thuận của khách hàng đối với nội dung giao dịch, thông điệp bằng phương thức điện tử rất phổ biến, tiết kiệm chi phí cho khách hàng và ngân hàng, thúc đẩy chính sách chuyển đổi số.

Dự thảo Thông tư bổ sung các quy định về hình thức xác nhận bằng phương tiện điện tử để thể hiện sự chấp thuận của khách hàng đối với giao dịch trực tuyến, bao gồm các hình thức xác thực giao dịch đã quy định tại Quyết định 630/QĐ-NHNN và Quyết định 2345/QĐ-NHNN.

1. Quy định về tiêu chuẩn xác thực bằng dấu hiệu nhận dạng sinh trắc học

Hiện nay, nhiều tổ chức tín dụng, trung gian thanh toán đã triển khai giải pháp định danh, xác minh khách hàng trực tuyến (eKYC) bằng dấu hiệu sinh trắc học. Tuy nhiên tại Việt Nam chưa có tiêu chuẩn kỹ thuật quy định về nội dung này. Cục CNTT đã khảo sát tình hình triển khai xác thực sinh trắc học tại các đơn vị trong ngành và tham khảo các tiêu chuẩn quốc tế và đề xuất bổ sung quy định về tiêu chuẩn xác thực bằng dấu hiệu nhận dạng sinh trắc học.

1. Bổ sung quy định về bảo vệ dữ liệu cá nhân của khách hàng theo quy định của pháp luật (Nghị định 13/2023/NĐ-CP của Chính phủ về bảo vệ dữ liệu cá nhân).
2. Bổ sung một số quy định mới để tăng cường bảo đảm an toàn, bảo mật, phòng ngừa các sự cố an toàn thông tin xảy ra trong thời gian gần đây như: Quy định về triển khai giải pháp tường lửa bảo vệ cơ sở dữ liệu; quy định về kiểm tra, gia cố an toàn, bảo mật (hardening) cho hệ thống Online Banking; quy định về việc cung cấp ứng dụng Mobile Banking trên các kho ứng dụng chính thức của các hãng cung cấp hệ điều hành cho thiết bị di động; quy định không gửi tin nhắn, thư điện tử cho khách hàng có nội dung chứa đường dẫn truy cập các trang điện tử, trừ trường hợp theo yêu cầu của khách hàng./.

**CỤC CÔNG NGHỆ THÔNG TIN**

1. Quyết định số 630/QĐ-NHNN ngày 31/3/2017 của Thống đốc NHNN về việc 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. [↑](#footnote-ref-1)
2. Quyết định 2345/QĐ-NHNN ngày 18/12/2023 của Thống đốc NHNN ban hành về triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng. [↑](#footnote-ref-2)