



# NHẬN DIỆN VÀ PHÒNG, CHỐNG HÀNH VI GIAN LẬN NGÂN HÀNG ĐIỆN TỬ TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ

Hà Lê Thủy

Trường Đại học Luật, Đại học Huế, Đường Võ Văn Kiệt, TP Huế, Việt Nam

\* Tác giả liên hệ: **Hà Lê Thủy** <hlthuy@hueuni.edu.vn >

(Ngày nhận bài: 29-05-2024; Ngày chấp nhận đăng: 11-12-2024)

**Tóm tắt.** Gian lận ngân hàng điện tử là một vấn đề đang xảy ra trên toàn cầu và đang tiếp tục gây tổn kém cho cả hệ thống ngân hàng và khách hàng. Gian lận ngân hàng điện tử xảy ra do nhiều nguyên nhân khác nhau như vi phạm về bảo mật, hệ thống xác thực yếu hay không đảm bảo về kiểm soát nội bộ. Mục đích của bài viết là làm rõ hành vi và các cách thức gian lận phổ biến hiện nay xảy ra trong lĩnh vực ngân hàng, đặc biệt là trong bối cảnh chuyển đổi số. Trên cơ sở phân tích, đánh giá các quy định của pháp luật, bài viết cũng cho thấy rằng, ngoài yếu tố trang bị công nghệ cao để giúp phát hiện hành vi gian lận, các yếu tố khác cũng cần phải được xem xét và chú trọng như kiểm soát nội bộ, tăng cường nhận thức của khách hàng về tính bảo mật dữ liệu cá nhân. Đây cũng chính là những giải pháp nhằm hướng tới việc phòng chống gian lận trong lĩnh vực ngân hàng nói chung và ngân hàng điện tử nói riêng.

**Từ khóa:** gian lận, ngân hàng điện tử, không gian mạng, tội phạm, chuyển đổi số

## IDENTIFY AND PREVENT FRAUDULENT ACTS ELECTRONIC BANKING IN THE CONTEXT OF DIGITAL TRANSFORMATION

**Ha Le Thuy**

University of Law, Hue University, Vo Van Kiet St., Hue City, Vietnam

Correspondence to **Ha Le Thuy** <hlthuy@hueuni.edu.vn>

(Received: May 29, 2024; Accepted: December 11, 2024)

**Abstract.** Electronic banking fraud is a global problem and continues to be costly to the banking system and customers. E-banking fraud occurs due to many different reasons, such as security violations, weak

---

authentication systems, or lack of internal control. The article aims to clarify fraud and common fraud methods currently occurring in the banking sector, especially in the context of digital transformation. Based on the analysis and evaluation of legal regulations, the article also shows that, in addition to the factor of high-tech equipment to help detect fraudulent acts, other factors also need to be considered and focus on internal control, increasing customer awareness about personal data security. These are also solutions aimed at preventing fraud in the banking sector in general and electronic transactions of banks in particular.

**Keywords:** fraud, electronic banking, cyberspace, crime, digital transformation.

## 1. Mở đầu

Chuyển đổi số mang lại nhiều lợi ích cho ngành ngân hàng, tài chính vì giúp các ngân hàng mở rộng thị trường, giảm chi phí quản lý, điều hành, nâng cao tỷ suất, hiệu quả kinh doanh qua các sản phẩm chuyển đổi số<sup>1</sup>. Chuyển đổi số được coi là yếu tố thúc đẩy và đưa ra giải pháp cho những thách thức mà các ngân hàng đang gặp phải trong kỷ nguyên số<sup>2</sup>. Hơn nữa, theo Terrar thì chuyển đổi số là quá trình mà một tổ chức phải trải qua khi thay đổi từ cách tiếp cận lỗi thời sang cách làm việc và tư duy mới bằng cách sử dụng kỹ thuật số, xã hội hóa, di động và công nghệ mới<sup>3</sup>. Nhưng bên cạnh đó, chuyển đổi số cũng khiến cho những hành vi vi phạm pháp luật nảy sinh, tồn tại và phát triển, các hình thức phạm tội mới ra đời với thủ đoạn tinh vi, phức tạp, lợi dụng sự phát triển của chuyển đổi số trong hệ thống ngân hàng để thực hiện các hành vi chiếm đoạt tài sản, gây ảnh hưởng, thất thoát, thiệt hại cho toàn hệ thống ngân hàng, gây rủi ro và thiệt hại cho các khách hàng đã trao niềm tin vào các ngân hàng.

Trong quá trình chuyển đổi số ngành ngân hàng, thuật ngữ ngân hàng điện tử ra đời và được thể hiện thông qua các hình thức khác nhau. Ngân hàng điện tử (tên tiếng anh là E-banking, Cyber Banking, Home Banking và Virtual Banking) bao gồm: Internet Banking, Mobile Banking, RTGS, ATM, Thẻ tín dụng, Thẻ ghi nợ, Thẻ thông minh... Theo Sathye, ngân hàng điện tử là việc cung cấp các dịch vụ ngân hàng qua internet, mang lại nhiều lợi ích tiềm năng cho việc áp dụng phương thức giao dịch mới này vào các tổ chức tài chính, đặc biệt sử dụng các công nghệ thân thiện với người dùng và giảm các hạn chế về vị trí hoặc khu vực địa lý. Đây là một loại phương tiện sinh lời tốt cho các tổ chức tài chính, đồng thời đem đến các dịch vụ tiện ích với tính linh hoạt và thoải mái hơn so với hệ thống ngân hàng truyền thống. Chính vì vậy, trong những năm qua, ngành ngân hàng trực tuyến đã phát triển nhanh chóng và sẽ tiếp tục

---

<sup>1</sup> Ngọc Bích, *Chuyển đổi số trong ngành tài chính-ngân hàng: Căn thuận tiện, an toàn*, truy cập tại: <https://www.vietnamplus.vn/chuyen-doi-so-trong-nganh-tai-chinhngan-hang-can-thuan-tien-an-toan/682629.vnp>, truy cập ngày 10/5/2022.

<sup>2</sup> Matt, C., Hess, T., & Benlian, A. (2015), *Digital transformation strategies*, *Business & information systems engineering*, 57(5), 339–343.

<sup>3</sup> Terrar, D (2015), *What is Digital Transformation?*, truy cập tại: <<http://www.theagileelephant.com/what-is-digitaltransformation/>>.

tăng trải nghiệm khi các tổ chức tài chính khuyến khích khách hàng sử dụng dịch vụ ngân hàng trực tuyến. Tuy nhiên, sự gia tăng của ngân hàng điện tử cùng với các dịch vụ tiện ích đang đứng trước nguy cơ phải đối mặt với nhiều rủi ro và thách thức do các cuộc tấn công và nguy cơ gian lận (lừa đảo) xâm nhập dữ liệu. Điều này đã làm giảm sự tin tưởng của người tiêu dùng vào khả năng tổ chức ngân hàng tài chính để bảo vệ họ cũng như lo lắng về sự an toàn đồng tiền của họ<sup>4</sup>.

Từ những tiện ích có được của ngân hàng điện tử, đồng thời từ những nguy cơ đối mặt với những gian lận xảy ra trong lĩnh vực ngân hàng, điều này dẫn đến các vấn đề được đặt ra và cần làm rõ, đó là: các hành vi gian lận ngân hàng điện tử là gì?; có những phương thức nào phổ biến hiện nay của gian lận ngân hàng điện tử?; pháp luật đã có những quy định kịp thời và đầy đủ để bảo vệ quyền lợi cho các chủ thể và ngăn ngừa các rủi ro khi hành vi gian lận xảy ra hay chưa? Những vấn đề này sẽ được giải quyết trong các nội dung dưới đây.

## 2. Khái niệm gian lận và hành vi gian lận ngân hàng điện tử

Về mặt ngữ nghĩa, gian lận có nguồn gốc Latin “*fraus*”, trong tiếng Anh là “*fraud*”. *Gian lận* là một dạng hành vi cố ý lừa dối nhằm đạt tới những mục đích hoặc nhu cầu của cá nhân hoặc tổ chức. Gian lận được hiểu là sự không trung thực, sự lừa dối có chủ ý, hoặc cố ý xuyên tạc sự thật, sự nói dối, sự cố ý nhắc lại những sự việc không có thật nhằm đạt được một lợi thế không công bằng hoặc gây bất lợi cho người khác<sup>5</sup>. Như vậy, gian lận đồng nghĩa với sự lừa dối, thiếu trung thực có ý thức, chống lại một người hoặc tổ chức để có được một số lợi thế nhất định. Hiểu theo nghĩa khái quát, gian lận là một phương pháp lấy tiền bất hợp pháp từ một người hoặc tổ chức, thường sử dụng các phương pháp thông minh và phức tạp, hay gian lận là chiếm đoạt hoặc sử dụng trái phép các quỹ hoặc hàng hóa được giao phó, giam giữ hoặc dưới sự kiểm soát của một người. Gian lận bao gồm một loạt các hành vi bất hợp pháp liên quan đến cố ý lừa dối hoặc xuyên tạc. Framework (IPPF) định nghĩa gian lận là: “Bất kỳ hành vi bất hợp pháp nào có đặc điểm là lừa dối, che giấu hoặc vi phạm của sự tin cậy. Những hành vi này không phụ thuộc vào sự đe dọa bạo lực hoặc vũ lực. Gian lận được thực hiện bởi các bên và tổ chức để có được tiền, tài sản hoặc dịch vụ để tránh thanh toán hoặc mất dịch vụ hoặc để đảm bảo lợi ích cá nhân hoặc kinh doanh”<sup>6</sup>. Còn theo Bhasin, “Gian lận thường diễn ra trong môi trường hệ thống tài chính khi các biện pháp bảo vệ và kiểm soát theo thủ tục không đầy đủ hoặc khi chúng không được tuân thủ một cách cẩn thận, do đó, khiến hệ thống dễ bị tổn thương

---

<sup>4</sup> Yazdanifard, Rashad, et al. (2011), *Electronic banking fraud: The need to enhance security and customer trust in online banking*, Advances in Information Sciences and Service Sciences, 3.10 (2011), p.505.

<sup>5</sup> Đỗ Thanh Bình, *Tìm hiểu lý thuyết tội phạm học về phòng ngừa tội phạm kinh tế và trong lĩnh vực ngân hàng*, truy cập tại: <http://congan.travinh.gov.vn/ch26/275-Tim-hieu-ly-thuyet-toi-pham-hoc-ve-phong-ngua-toi-pham-kinh-te-va-trong-linh-vuc-ngan-hang.html>, truy cập ngày 01/5/2022.

<sup>6</sup> Institute of Internal Auditors (2009), International Professional Practices Framework, IIA.

bởi những kẻ phạm tội”<sup>7</sup>. Quan điểm của Adewumi lại cho rằng, gian lận là một hành động có ý thức từ trước của một người hoặc một nhóm người với ý định thay đổi sự thật và/hoặc thực tế vì lợi ích tài sản cá nhân. Nó liên quan đến việc sử dụng thủ đoạn lừa dối, thậm chí đôi khi rất tinh vi và có sự tính toán một cách kĩ lưỡng như giả mạo, làm sai lệch tài liệu và ủy quyền chữ ký hay một hành vi trộm cắp có chủ đích<sup>8</sup>.

Trong khi đó, dù chưa có định nghĩa chính thức về gian lận ngân hàng nhưng có thể hiểu rằng, gian lận ngân hàng là việc sử dụng các phương tiện có khả năng bất hợp pháp để có được tiền, tài sản hoặc của cải khác được sở hữu hoặc nắm giữ bởi một tổ chức tài chính, hoặc để có được tiền từ người gửi tiền bằng cách giả bộ một cách gian lận như là một ngân hàng hoặc tổ chức tài chính khác. Gian lận ngân hàng là việc cố ý xuyên tạc (thường đòi hỏi một số chuyên môn kỹ thuật) để lừa đảo. Các loại gian lận mà tổ chức tài chính thường gặp bao gồm gian lận bán hàng, gian lận mua hàng, gian lận thanh toán bằng séc và gian lận ATM lấy tiền hoặc các tài sản khác từ ngân hàng<sup>9</sup>.

Trong ngân hàng điện tử, gian lận là yếu tố góp phần chính vào thuật ngữ bảo mật và cần được quản lý chặt chẽ. Gian lận ngân hàng có sử dụng công nghệ cao hoặc sử dụng mạng internet chính là một hình thức gian lận ngân hàng điện tử. Đó là bất kỳ biểu hiện thiếu sót hoặc che giấu nào được tính toán nhằm đánh lừa người khác, gây bất lợi cho người đó và được thực hiện thông qua việc sử dụng máy tính hoặc thông tin liên lạc điện tử trong quá trình giao dịch điện tử. Có quan điểm cho rằng bản chất của gian lận cũng chính là lừa đảo vì lừa đảo là một trong những cơ chế mà những kẻ lừa đảo sử dụng để lấy thông tin cá nhân của khách hàng dẫn đến việc sử dụng nó cho các hoạt động gian lận<sup>10</sup>. Với cách hiểu như vậy, có thể thấy rằng lừa đảo cũng là một hình thức của gian lận, do đó, hành vi gian lận có sử dụng công nghệ cao hay còn gọi là gian lận trực tuyến chính là một hình thức lừa đảo trực tuyến. Chính vì vậy, trong nghiên cứu của mình, Tan đã cho rằng, lừa đảo trực tuyến có thể được thực hiện trong các phòng chat chuyển tiếp internet qua thư điện tử bản tin hoặc trên các trang web theo đó những người sử dụng internet có khả năng sử dụng internet và thực hiện các giao dịch trực tuyến có khả năng là nạn nhân dễ bị lừa đảo<sup>11</sup>. Như vậy có thể thấy rằng, gian lận được hiểu bao gồm cả giả mạo hoặc sai sót và thậm chí là lừa đảo. Sự giả mạo chính là viết sai hoặc sửa chữa giấy tờ, văn bản với ý định lừa gạt. Trong khi đó, lừa đảo là các thủ thuật được tội phạm mạng và kẻ lừa đảo áp dụng để khiến nạn nhân tiết lộ thông tin tài chính cá nhân và bí mật khác. Chúng tôi

---

<sup>7</sup> Bhasin, M. L. (2016), Contribution of Forensic Accounting to Corporate Governance: An Exploratory Study of an Asian Country, *International Business Management*, 10(4), 479–492.

<sup>8</sup> Adewumi, W. (1986), *Fraud in Banks*, Nigeria Institute of Bankers.

<sup>9</sup> Benjamin, O.A. & Samson, B.S. (2011), Effect of perceived inequality and perceived jobinsecurity on fraudulent intent of bank employees in Nigeria, *Europe's Journal of Psychology*, 7(1), 99–111.

<sup>10</sup> Usman, Ahmad Kabir, and Mahmood Hussain Shah (1970), Critical success factors for preventing e-banking fraud, *The Journal of Internet Banking and Commerce*, 18.2, 1–14.

<sup>11</sup> Tan, H. S. (2002), E-Fraud: Current Trends and International Developments, *Journal of Financial Crime*, 9(4), p.348.

cho rằng, lừa đảo trực tuyến liên quan đến hệ thống các ngân hàng cũng chính là một hình thức gian lận trực tuyến trong lĩnh vực ngân hàng hay còn gọi là gian lận ngân hàng điện tử<sup>12</sup>.

Tóm lại, *gian lận ngân hàng điện tử* chính là hành vi sử dụng các phương tiện điện tử trên nền tảng trực tuyến tạo ra các thủ đoạn gian dối để thực hiện các giao dịch trong lĩnh vực ngân hàng một cách trái pháp luật nhằm chiếm đoạt tài sản hoặc nhằm mục đích vụ lợi khác. Hành vi gian lận ngân hàng điện tử tác động đến hệ thống ngân hàng, gây ảnh hưởng đến các hoạt động trực tuyến và gây ra các thiệt hại cho chính các ngân hàng cũng như cho các khách hàng đã trao gửi niềm tin vào ngân hàng.

### 3. Nhận diện các hành vi gian lận ngân hàng điện tử

Trong các tài liệu nước ngoài, gian lận ngân hàng có nhiều hình thức khác nhau. Chẳng hạn như gian lận tổng hợp, gian lận công ty, gian lận điều hành, gian lận nội bộ, gian lận bên ngoài, gian lận máy tính, gian lận hỗ trợ lãnh đạo, gian lận được hỗ trợ tư pháp...<sup>13</sup> hay các loại gian lận trộm cắp và tham ô, làm sai lệch, giả mạo, gian lận thay thế, cho vay trái phép, vay không chính thức, mạo danh, lập hóa đơn quá mức, thao túng chứng từ, hợp đồng hư cấu, tài khoản hư cấu, định giá quá cao/thấp hơn định giá tài sản, kê khai khống tiến mặt thiếu hụt, sử dụng gian dối tài liệu ngân hàng, làm sai lệch báo cáo trạng thái, lạm dụng tài khoản tạm ngưng, chuyển thư, chặn thanh toán bù trừ kiểm tra, rửa tiền, gian lận máy tính, thu tiền sai<sup>14</sup>.

Trong các loại hình nói trên, có thể thấy gian lận có sự hỗ trợ của máy tính hoặc các loại thiết bị điện tử (sau đây gọi chung là máy tính) chính là một dạng cụ thể của gian lận ngân hàng điện tử. Đây là một quá trình liên quan đến tất cả các hành vi, liên quan đến việc sử dụng máy tính thông qua cách thức hoặc cách tiếp cận gian dối hoặc không trung thực để tước đoạt quyền của cá nhân hoặc tài sản của họ mà không có sự đồng ý của họ. Ở đây, máy tính là đối tượng chính của gian lận. Máy tính được xem như một công cụ được tội phạm sử dụng để thực hiện hành vi gian lận thông qua thao tác nhập dữ liệu, thao tác chương trình hoặc thao tác hoạt động như: giả mạo các tệp máy tính; thao tác dữ liệu đầu vào; tạo tài khoản hư cấu; sử dụng mật khẩu của nhân viên khác; sử dụng các ứng dụng giả; sử dụng mật khẩu chính. Theo Owolabi, ngân hàng điện tử cũng thu hút nhiều loại gian lận như bị đánh cắp thẻ (gian lận thẻ thực tế), các ứng dụng gian lận, gian lận thao tác dữ liệu thẻ, thư rác hoặc từ chối dịch vụ, gian lận truy cập nhanh chóng, gian lận chuyển tiền, gian lận thanh toán bù trừ liên ngân hàng, gian lận rửa tiền và thư lừa đảo<sup>15</sup>.

---

<sup>12</sup> Xem thêm Hà Lê Thủy (2022), Gian lận ngân hàng điện tử – Một dạng hành vi phạm tội mới trong bối cảnh chuyển đổi số ngành Ngân hàng, *Tạp chí Ngân hàng*, số chuyên đề đặc biệt, tr.102.

<sup>13</sup> Ojo, A. (2006), *Curbng Fraud within the Banking System: A banker's Perspectives*, Lagos: A.M. Continental Ltd.

<sup>14</sup> Owlo, O. (2005), *Bank Frauds, Causes and Prevention: An Empirical Analysis*, Ibadan: ATT Books Ltd.

<sup>15</sup> Owolabi, S. A (2010), *Fraud and fraudulent practices in Nigeria banking industry*, African Research Review 4.3.

Trong khi đó theo Dzomira, gian lận điện tử có thể được phân thành hai loại: gian lận trực tiếp và gian lận gián tiếp. Gian lận trực tiếp bao gồm gian lận thẻ tín dụng/thẻ ghi nợ, nhân viên biển thủ, rửa tiền. Gian lận gián tiếp bao gồm lừa đảo, hack, vi rút, thư rác, phí ứng trước và phần mềm độc hại. Gian lận thẻ tín dụng/thẻ ghi nợ và trộm cắp danh tính là hai hình thức gian lận điện tử thường được sử dụng thay thế cho nhau. Nó liên quan đến việc mạo danh và trộm cắp danh tính (tên, số bảo hiểm xã hội (SIN), số thẻ tín dụng hoặc thông tin nhận dạng khác) để thực hiện các hoạt động gian lận<sup>16</sup>.

Ở Việt Nam, các nghiên cứu về gian lận ngân hàng điện tử còn rất ít, chưa có một tài liệu thống kê chính thức nào về hình thức gian lận trong lĩnh vực ngân hàng điện tử phổ biến đang xảy ra hiện nay. Tuy nhiên, trong các cuộc hội thảo tổ chức ở Việt Nam, các chuyên gia đã nhận định rằng, tại Việt Nam kẻ gian thường sử dụng 4 phương thức gian lận phổ biến như: Đánh cắp thông tin và tấn công mạng (Phishing and Cyber Attacks); sử dụng phần mềm, ứng dụng độc hại (Malware, Ransomware); tấn công phi kỹ thuật (Social Engineering); rủi ro gian lận nội bộ (Insider Threats). Ngoài ra, hành vi gian lận được thể hiện ở việc tội phạm công nghệ cao kết hợp giữa hai hình thức phishing (tấn công giả mạo) và social engineering (tấn công phi kỹ thuật) gồm các mảnh khoé, kỹ thuật tấn công nhằm vào bản tính xã hội của con người, thông qua tác động trực tiếp lên tâm lý con người, chứ không thuộc về máy móc. Khi tội phạm có thể thuần thục cả hai phương thức này thì khá dễ dàng trong việc lừa đảo hòng chiếm đoạt tài khoản ngân hàng qua các thông tin, dữ liệu cá nhân bị lộ, lọt, từ đó thực hiện các giao dịch giả mạo, chiếm đoạt tiền trong tài khoản của khách hàng. Tuy cách thức thực hiện gian lận có thể khác nhau, nhưng đều chung mục đích chiếm đoạt tiền, tài sản hoặc thông tin cá nhân nhạy cảm, từ đó gây tác động tiêu cực đến người tiêu dùng, doanh nghiệp bán hàng lẫn các tổ chức tài chính.

Từ đây, để nhận diện hình thức gian lận ngân hàng điện tử (hay còn gọi là lừa đảo công nghệ cao, gian lận ngân hàng trong môi trường số) ở Việt Nam hiện nay, có thể thấy có các hình thức như sau:

- Đánh cắp thông tin bảo mật để chiếm quyền sử dụng thẻ hoặc tài khoản ngân hàng điện tử.
- Lừa đảo khách hàng tự thực hiện giao dịch gian lận, chẳng hạn như kẻ gian lừa khách hàng tự thực hiện giao dịch chuyển tiền cho mình.
- Trộm cắp danh tính: kẻ gian sử dụng trái phép thông tin cá nhân của khách hàng để đăng ký mở tài khoản, đăng ký dịch vụ ngân hàng điện tử của khách hàng để chiếm quyền sử dụng, đăng ký vay trực tuyến, hoặc sử dụng vào các mục đích gian lận bất chấp việc ngân hàng

---

<sup>16</sup> Dzomira, S. (2014), Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe, *Risk Governance and Control: Financial Markets and Institutions*, 4(2), 16–26.

đã áp dụng các giải pháp công nghệ bảo mật mới nhất và thường xuyên cảnh báo tới khách hàng cần bảo mật thông tin trong quá trình giao dịch.

Để có được dữ liệu cá nhân của khách hàng, kẻ gian có thể sử dụng các thủ đoạn như sau:

- Lừa đảo qua email: sử dụng email có chứa một liên kết mà khi nhấp vào đó sẽ đưa đến một trang web giả mạo giống với trang web của ngân hàng mà nạn nhân có liên kết với ngân hàng đó, sau khi nạn nhân khai thông tin cá nhân vào trang web này, kẻ lừa đảo đã đánh cắp thông tin đó và sử dụng để rút tiền trái phép từ tài khoản ngân hàng của người này.

- Lừa đảo giả mạo nhân viên ngân hàng: giả danh một nhân viên của ngân hàng để yêu cầu khách hàng cung cấp thông tin cá nhân, sau đó sử dụng thông tin này để truy cập vào tài khoản cá nhân của người này và thực hiện các giao dịch rút tiền trái phép.

- Sử dụng phần mềm độc hại để lừa đảo: làm lây nhiễm phần mềm độc hại vào máy tính cá nhân của các khách hàng và thực hiện việc rút tiền tài khoản sau đó.

- Lừa đảo tâm lý: dựa trên việc cung cấp các khoản vay nhanh chóng và dễ dàng hoặc lừa đảo tuyển dụng với việc đăng danh sách việc làm giả lên mạng.

Dựa vào các hình thức gian lận và thủ đoạn gian lận nói trên, có thể thấy có nhiều nguyên nhân dẫn đến hành vi gian lận ngân hàng điện tử bởi lẽ như đã nói, môi trường internet đã trở thành mảnh đất màu mỡ cho những kẻ lừa đảo nhắm tới người tiêu dùng. Nó cho phép tội phạm có khả năng xuất hiện bất ngờ lừa gạt nhanh chóng rồi biến mất mà không tiết lộ danh tính hoặc địa điểm thực sự của chúng. Các nguyên nhân này có thể là những nguyên nhân phát sinh và gia tăng tội phạm công nghệ cao trong các lĩnh vực của xã hội nói chung hay gian lận trong lĩnh vực ngân hàng nói riêng.

Nguyên nhân trước hết phải kể đến đó là yếu tố công nghệ. Sự sẵn có dễ dàng của các công nghệ mới với tốc độ hoạt động, năng lực và khả năng kết nối cao giúp các hoạt động bất hợp pháp dễ dàng thoát khỏi sự phát hiện. Ngược lại, phần lớn nạn nhân của tội phạm công nghệ cao không có kiến thức về công nghệ hoặc không có các thiết bị công nghệ tân tiến đủ để ngăn chặn, phát hiện hoặc đối phó với loại tội phạm này. Người dùng ngày càng phụ thuộc vào các sản phẩm và dịch vụ trực tuyến, trong khi các ngân hàng đang chuyển sang hoạt động trực tuyến để đáp ứng nhu cầu thị trường. Tuy nhiên, sự phát triển của kinh doanh trực tuyến cùng với sự tinh vi ngày càng tăng của tội phạm công nghệ bên cạnh mức độ hiểu biết và kiến thức chung của người dùng về các quy trình bảo mật nói chung còn thấp đã tạo ra một môi trường thay thế tối ưu cho hành vi gian lận. Trong lĩnh vực ngân hàng hiện nay chưa thực sự có nền tảng công nghệ hoàn chỉnh và đồng bộ để hỗ trợ công tác quản trị rủi ro gian lận. Hệ thống phát hiện gian lận không đủ linh hoạt để ứng phó với sự thay đổi hình thái gian lận một cách nhanh chóng.

Bên cạnh đó, vấn đề nhận thức rủi ro và bảo mật thông tin để giảm thiểu rủi ro cũng còn thấp đối với các chủ là các tổ chức tài chính hay các cơ quan thực thi pháp luật, cơ quan bảo vệ pháp luật. Sự thiếu nhận thức về cách duy trì mức độ bảo mật tối thiểu đối với thông tin cá nhân hoặc tài sản điện tử, sự thiếu chú trọng giáo dục để nâng cao nhận thức khiến cho tình hình gian lận phát sinh và gia tăng là điều khó tránh khỏi. Trong một số trường hợp khi phát hiện tội phạm, các tổ chức ngân hàng ngần ngại báo cáo hoạt động tội phạm vì lo ngại việc công khai có thể gây xấu hổ, mất niềm tin của công chúng, mất nhà đầu tư hoặc ảnh hưởng kinh tế. Điều này khiến cho cơ hội xảy ra gian lận cũng tăng theo.

#### **4. Khuôn khổ pháp luật Việt Nam về phòng chống gian lận ngân hàng điện tử**

Trong khuôn khổ pháp lý quốc tế, các quốc gia trên thế giới cũng đã nỗ lực bắt tay cùng nhau kí kết các văn bản pháp lý để phòng chống tội phạm mạng nói chung, trong đó có tội phạm liên quan đến lĩnh vực ngân hàng. Bởi lẽ, bảo vệ an toàn, an ninh mạng, phòng chống các loại tội phạm mạng, tội phạm sử dụng công nghệ cao, đã trở thành cấu phần then chốt trong chiến lược an ninh của nhiều quốc gia. Ở châu Âu, các nước cũng đã có những chính sách và chiến lược chống lại tội phạm công nghệ cao. Các tổ chức này đã liên kết với nhau vì có cùng chung quan điểm và mối quan tâm hàng đầu đến tội phạm công nghệ cao. Hội đồng châu Âu (EU) cũng đã thành lập ủy ban chuyên gia về tội phạm trong không gian mạng vào tháng 2/1997, sau đó đã đi đến cuộc họp về “hỗ trợ lẫn nhau trong cuộc chiến chống lại tội phạm tham nhũng, rửa tiền, tội phạm công nghệ cao, bóc lột tình dục, tội phạm có tổ chức” để ban hành công ước của Hội đồng châu Âu về tội phạm mạng.

Ở khuôn khổ trong nước, từ trước đến nay, Việt Nam cũng đã nỗ lực ban hành các văn bản có liên quan để điều chỉnh hoạt động của ngân hàng nói chung và ngân hàng điện tử nói riêng. Có thể kể đến các văn bản như: Luật ngân hàng nhà nước năm 2010, Luật các tổ chức tín dụng năm 2010 sửa đổi năm 2017, Luật An toàn thông tin mạng năm 2015, Luật An ninh mạng năm 2018, Luật Giao dịch điện tử năm 2023. Trong phạm vi toàn ngành ngân hàng, để đảm bảo an toàn cho hoạt động thanh toán điện tử, Ngân hàng Nhà nước đã ban hành Chỉ thị 02/CTNHNN về đẩy mạnh chuyển đổi số và bảo đảm an ninh, an toàn thông tin trong hoạt động ngân hàng. Trên cơ sở đó, các ngân hàng chấp hành nghiêm túc các quy định của Ngân hàng Nhà nước về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên internet (theo Thông tư 29/2011/TT-NHNN ngày 21/9/2011); quy định các yêu cầu kỹ thuật về an toàn bảo mật đối với trang thiết bị phục vụ thanh toán thẻ ngân hàng (theo Thông tư 47/2014/TT-NHNN ngày 31/12/2014); quy định về bảo đảm an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng (theo Thông tư 31/2015/TT-NHNN ngày 28/12/2015); quy định việc trang bị, quản lý, vận hành và bảo đảm an toàn hoạt động của máy giao dịch tự động (theo Thông tư 36/2012/TT-NHNN ngày 28/12/2012; Thông tư 20/2016/TT-NHNN ngày 30/6/2016)



cũng như các văn bản chỉ đạo khác của Ngân hàng Nhà nước về hoạt động thanh toán nói chung, thanh toán thẻ, thanh toán điện tử.

Đồng thời với đó, Việt Nam ban hành các văn bản về phòng chống các hành vi sử dụng không gian mạng để phạm tội như: Luật xử lý vi phạm hành chính năm 2012, Bộ luật hình sự năm 2015 sửa đổi, bổ sung năm 2017, Nghị định số 25/2014/NĐ-CP ngày 07/04/2014 quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao, Nghị định số 88/2019/NĐ-CP ngày 14/11/2019 quy định về xử phạt vi phạm hành chính trong lĩnh vực tiền tệ và ngân hàng. Gần đây nhất, Thủ tướng Chính phủ đã ban hành Chỉ thị 21/CT-TTg ngày 25/5/2020 về tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản, trong đó đặc biệt nhấn mạnh đến lừa đảo chiếm đoạt tài sản trên không gian mạng. Ở mức độ xử lý hình sự đối với các hành vi gian lận trong lĩnh vực ngân hàng, Bộ luật hình sự năm 2015 đã quy định các tội phạm có liên quan mà việc áp dụng một trong số các tội phạm này tùy thuộc vào ý thức của kẻ phạm tội và mục đích của việc phạm tội. Đó là các tội: Tội trộm cắp tài sản (Điều 173), tội lừa đảo chiếm đoạt tài sản (Điều 174), tội vi phạm quy định về hoạt động ngân hàng, hoạt động khác liên quan đến hoạt động ngân hàng (Điều 206) hoặc tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản (Điều 290). Tuy nhiên có thể thấy rằng, việc xử lý hình sự bằng các trường hợp phạm tội kể trên vẫn chưa đáp ứng được nhu cầu đấu tranh phòng ngừa và xử lý tội phạm gian lận trong lĩnh vực ngân hàng bởi lẽ, mỗi tội đặc trưng cho một dấu hiệu nhất định mà không thể hiện rõ và đầy đủ các dấu hiệu của hành vi gian lận ngân hàng điện tử như: tính chất gian lận của hành vi; phương thức thực hiện hành vi phạm tội thông qua không mạng; hành vi liên quan trực tiếp đến ngân hàng; mục đích chiếm đoạt tài sản hoặc mục đích xâm hại đến lĩnh vực ngân hàng và gây ra thiệt hại cho các khách hàng, hệ thống ngân hàng. Ngoài ra cho đến hiện tại, Việt Nam chưa có Luật phòng chống tội phạm công nghệ cao mà mới chỉ có Nghị định số 25/2014/NĐ-CP ngày 07/04/2014 quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao như đã kể trên. Vì thế, những quy định pháp luật nói trên vẫn mang tính manh mún, tản mạn, các quy định điều chỉnh hoạt động của ngân hàng điện tử còn chưa đầy đủ và đồng bộ, cơ chế xử lý hành vi vi phạm còn chưa tương xứng với tính chất và mức độ nguy hiểm cho xã hội của hành vi xâm phạm đến hoạt động của ngân hàng điện tử. Vì vậy, có thể thấy rằng, Việt Nam chưa có cơ sở pháp lý đủ mạnh để phòng ngừa và xử lý các hành vi vi phạm trên không gian mạng, trong đó bao gồm cả hành vi gian lận ngân hàng điện tử.

## **5. Các giải pháp phòng chống gian lận ngân hàng điện tử**

Xu hướng và tiềm năng phát triển của ngân hàng điện tử đặt ra nhiều thách thức cho các nhà quản lý trong việc thúc đẩy sự phát triển của ngân hàng điện tử, đồng thời phải bảo vệ quyền lợi khách hàng, đảm bảo an ninh hệ thống và dữ liệu khách hàng, tránh các rủi ro về

gian lận ngân hàng điện tử xảy ra. Để đạt được điều này, cần có các giải pháp trước mắt và lâu dài.

Thứ nhất, tiếp tục hoàn thiện các quy định pháp luật, sửa đổi bổ sung một số văn bản có liên quan đến lĩnh vực ngân hàng điện tử. Như trên đã phân tích, sự phát triển nhanh của sản phẩm và dịch vụ của ngân hàng điện tử làm cho hành lang pháp lý của Việt Nam còn nhiều quy định chưa tương thích, chưa thực sự thúc đẩy phát triển ngân hàng điện tử, thanh toán điện tử. Không những thế, áp lực gia tăng từ các cuộc tấn công an ninh mạng và lừa đảo ngày càng gia tăng khiến cho việc thực thi pháp luật về phòng ngừa, phát hiện và xử lý các hành vi nói trên chưa hiệu quả, thậm chí pháp luật chưa theo kịp sự phát triển của công nghệ. Do đó, Việt Nam cần sớm ban hành Luật phòng chống tội phạm công nghệ cao trong thời gian tới để có thể đồng bộ với những văn bản pháp luật trước đây nhằm điều chỉnh các hành vi vi phạm trong lĩnh vực ngân hàng nói chung và hành vi gian lận ngân hàng điện tử nói riêng.

Thứ hai, xây dựng và thiết lập hệ thống bảo mật thông tin của khách hàng, trong đó trách nhiệm bảo mật phải đến từ nhiều phía, ngân hàng chỉ là một trong số các chủ thể có trách nhiệm. Cùng với đó là việc giáo dục người tiêu dùng cần nhận thức và phải tự bảo vệ mình, không được dễ dãi trong việc chia sẻ thông tin cá nhân của mình khi thực hiện các giao dịch tài chính trên môi trường internet bởi lẽ môi trường internet luôn đi cùng với rủi ro và tội phạm mạng thì sẽ chỉ ngày càng tinh vi hơn. Đây cũng sẽ là một biện pháp có hiệu quả hơn bao giờ hết trong việc ngăn chặn hành vi gian lận được thực hiện thông qua ngân hàng điện tử.

Thứ ba, tăng cường năng lực cho đội ngũ thực thi pháp luật thông qua việc đào tạo về những công nghệ và bí quyết mới nhất về điều tra và truy tố các vụ gian lận ngân hàng điện tử. Những chương trình đào tạo này nên được tổ chức thường xuyên vì công nghệ máy tính phát triển nhanh chóng. Do sự phức tạp về kỹ thuật cùng với các vấn đề pháp lý nghiêm trọng do những tội phạm gây ra, nên mỗi khu vực pháp lý đang phát triển như Việt Nam cần có các đội chuyên gia, những người có thể cống hiến hết mình cho việc điều tra và thực thi pháp luật về phòng chống hành vi gian lận ngân hàng điện tử.

Thứ tư, cần liên tục triển khai các công nghệ chống gian lận mới nhất cho ngành ngân hàng. Chẳng hạn như tất cả thẻ ghi nợ và thẻ tín dụng sẽ được thay thế bằng thẻ thông minh có gắn vi mạch. Với công nghệ thẻ thông minh áp dụng phương thức xác minh chủ thẻ, cho phép xác minh giao dịch mua hàng thông qua mã số nhận dạng cá nhân giúp giao dịch an toàn hơn. Chẳng hạn như xác thực chủ thẻ bằng đầu đọc dấu vân tay và đầu đọc thẻ di động để giảm các giao dịch thẻ trực tuyến trái phép, điều này sẽ khiến cho máy chủ của người bán hàng cũng không biết thông tin và số thẻ thực của khách hàng. Đây có thể là một khó khăn khi khách hàng buộc phải thay đổi tư duy và cách tiếp cận sử dụng các tính năng thông minh về cách thức tiến hành các giao dịch ngân hàng. Tuy nhiên, đây lại là cách mà các nước phát triển trên thế giới đã tiến hành từ lâu, còn Việt Nam vốn chỉ được xem là ở thời kì đầu của quá trình số hóa ngành

ngân hàng. Vì vậy tiếp tục triển khai thực hiện các công cụ thông minh giúp tăng tính hiệu quả trong việc phòng ngừa gian lận ngân hàng điện tử là điều cần thiết.

## 6. Kết luận

Gian lận ngân hàng điện tử là một hình thức gian lận mới, khác với các hình thức gian lận truyền thống bởi lẽ được thực hiện thông qua các phương tiện không tiếp xúc, phương tiện truyền thông trực tiếp hay phương tiện thanh toán mới. Tuy nhiên, với sự cập nhật liên tục của các phương thức, thủ đoạn gian lận trong lĩnh vực ngân hàng trên không gian mạng, việc nhận diện hành vi gian lận ngày càng trở nên khó khăn hơn. Vì vậy, thông qua việc đưa ra các khái niệm, dấu hiệu, đặc điểm và phân loại các hành vi gian lận trong lĩnh vực ngân hàng điện tử, điều này có thể giúp ích cho việc nhận diện dấu hiệu pháp lý để xử lý hành vi gian lận cũng như việc ngăn ngừa và giảm thiểu rủi ro gian lận xảy ra. Hệ thống các ngân hàng ở Việt Nam đang trong quá trình chuyển đổi số và hoàn thiện dần về mọi mặt, trong khi hệ thống pháp luật điều chỉnh về vấn đề này cũng buộc phải theo kịp sự phát triển của khoa học công nghệ và dự liệu được các hành vi của tội phạm công nghệ cao phát sinh.

## TÀI LIỆU THAM KHẢO

1. Adewumi, W. (1986), *Fraud in Banks*, Nigeria Institute of Bankers.
2. Benjamin, O.A. & Samson, B.S. (2011), Effect of perceived inequality and perceived jobinsecurity on fraudulent intent of bank employees in Nigeria, *Europe's Journal of Psychology*, 7(1), 99–111.
3. Bhasin, M. L. (2016), Contribution of Forensic Accounting to Corporate Governance: An Exploratory Study of an Asian Country, *International Business Management*, 10(4), 479–492.
4. Ngọc Bích (2020), *Chuyển đổi số trong ngành tài chính-ngân hàng: Căn thuận tiện, an toàn*, truy cập tại: <https://www.vietnamplus.vn/chuyen-doi-so-trong-nganh-tai-chinhngan-hang-can-thuan-tien-an-toan/682629.vnp>, truy cập ngày 10/5/2022.
5. Đỗ Thanh Bình (2017), *Tìm hiểu lý thuyết tội phạm học về phòng ngừa tội phạm kinh tế và trong lĩnh vực ngân hàng*, truy cập tại: <http://congan.travinh.gov.vn/ch26/275-Tim-hieu-ly-thuyet-toi-pham-hoc-ve-phong-ngua-toi-pham-kinh-te-va-trong-linh-vuc-ngan-hang.html>, truy cập ngày 16/9/2023.
6. Dzomira, S. (2014), Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe, *Risk Governance and Control: Financial Markets and Institutions*, 4(2), 16–26.

7. Matt, C., Hess, T., & Benlian, A. (2015), Digital transformation strategies, *Business & information systems engineering*, 57(5), 339–343.
8. Ojo, A. (2006), *Curbing Fraud within the Banking System: A banker's Perspectives*, Lagos: A.M. Continental Ltd.
9. Owbo, O. (2005), *Bank Frauds, Causes and Prevention: An Empirical Analysis*, Ibadan: ATT Books Ltd.
10. Owolabi, S. A (2010), *Fraud and fraudulent practices in Nigeria banking industry*, *African Research Review* 4.3, 240–256.
11. Terrar, D. (2015), *What is digital transformation*, truy cập tại: <http://www.the-agile-elephant.com/what-is-digital-transformation.html>.
12. Hà Lê Thủy (2022), Gian lận ngân hàng điện tử – Một dạng hành vi phạm tội mới trong bối cảnh chuyển đổi số ngành Ngân hàng, *Tạp chí Ngân hàng*, số chuyên đề đặc biệt, tr.100–106.
13. Usman, Ahmad Kabir, and Mahmood Hussain Shah (1970), Critical success factors for preventing e-banking fraud, *The Journal of Internet Banking and Commerce*, 18.2, 1–14.
14. Yazdanifard, Rashad, et al. (2011), Electronic banking fraud: The need to enhance security and customer trust in online banking, *Advances in Information Sciences and Service Sciences*, 3.10 (2011), 505–509.