*IOSR Journal of Economics and Finance (IOSR-JEF)*
*e-ISSN: 2321-5933, p-ISSN: 2321-5925, Volume 16, Issue 4 Ser.1 (Jul. – Aug. 2025), PP 01-07*
*www.iosrjournals.org*

# Beyond Banking Apps: The Rise of Fraud Targeting Embedded Finance and Buy-Now-Pay-Later Services

**AUTHOR**

***Abstract***
*Fraud and cybercrime are now found in embedded finance and buy-now-pay-later (BNPL) as well as regular banking and this paper examines these shifts by looking at worldwide trends seen since 2020. Integrating banking products onto other applications is becoming much more popular (Bin Hendi, 2025). BNPL's popularity has also grown quickly: from $2.3 billion in e-commerce in 2014, its global share grew to $342 billion in 2024 and it is expected to reach $580 billion in 2030 (O'Connor, 2025; Malkoochi, 2025). Because of the scale and speed of cryptocurrency operations, fraudsters have taken notice. New studies indicate that fraud cases rose by about 60% in BNPL since 2021 (Malkoochi, 2025) and most frauds are now synthetic identity creation, account takeovers and misusing bank cards stolen from people. These cyber risks create new problems: attackers take advantage of convenient banking services supported by APIs to circumvent usual banking safety measures (Alloy, 2023; F5, 2021). Due to this, industry and regulators are particularly focused on strong identity checking, ML-driven detection and compliance (CFPB, 2022; OCC, 2023; Bello & Olufemi, 2024). This research reviews both academic and industry materials, focuses on main fraud areas and presents ways to protect against identity theft, hacking and group scams. The discussion looked at actual events (attacks against BNPL partners) and recent rules introduced in the UK and US to highlight how these matters impact cybersecurity. It seeks to chart new fraud threats and methods to prevent them because finance is being integrated into various applications.*

---

Date of Submission: 23-06-2025 Date of Acceptance: 04-07-2025

---

## I. Introduction

The payments world is being changed by embedded finance which is adding financial tools to popular applications and platforms (Bin Hendi, 2025). Incorporating payments, lending, insurance and similar services into retail apps and online sites is designed to simplify the way consumers make transactions. For example, a ride-hailing app might supply insurance or a buy now, pay later option directly and on a shopping site, customers could benefit from instant installment loans during checkout. Thanks to the partnership between fintech firms and banks, along with API and open banking, the sector is experiencing this transformation. It is projected by the World Economic Forum that embedded finance could be worth $7.2 trillion by 2030.

At the same time, Buy-Now-Pay-Later (BNPL) is now being used by many people globally to pay for purchases in installments. The industry claims that from only a few billion dollars in the mid-2010s, BNPL grew to be worth hundreds of billions by now, in e-commerce. The 2020 Worldpay Global Payments Report shows that BNPL rose from $2.3 billion in 2014 to $342 billion in 2024 and it expects the total to exceed $580 billion by 2030. This boom is being driven by consumers who want easy, free credit at checkout and retailers who agree to accept it. Nearly a tenth of all e-commerce in Europe is BNPL and Switzerland is highest at 22%, but growth is happening everywhere.

Though embedded finance and BNPL simplify access to credit and payments, their rising popularity introduces new security problems. Using old controls such as secure mobile apps and multi-factor authentication, was the main way banks spotted fraud. On the other hand, because embedded finance is designed for convenience such as easy credit checking and little data needed, this can make them more at risk. Fradusters are quick to see these openings. BNPL and embedded finance services have become major targets for criminals, according to financial industry analysts. For example, Alloy says that at launch, new financial services often come under attack due to their new controls that might be less secure. New customer on-boarding is no longer allowed by banking-as-a-service firms in Europe because of non-compliance, as proven by recent regulatory decisions.

This paper examines the threats to cybersecurity related to fraud in embedded finance and BNPL over the past two years. Different studies were analyzed and papers explaining how fraud schemes are now targeting these new fields, examine what attackers are doing and why and recommend safety strategies. Issues such as APIs, ID checks and the use of AI were carefully looked at and also the specific regulations for Buy Now, Pay

Later by US and UK regulators. Examples from across the world are offered to give a global view throughout the book. The structure is as follows: Section 2 examines what existing research and industry analysis have to say about embedded finance, BNPL trends and fraud. All this research is grouped into related threats and possible solutions in Section 3 (Discussion), mentioning helpful case studies where they are available. To wrap up, major cybersecurity challenges and how security can be made stronger as things develop were discussed.

## II. Literature Review

The Embedded Finance and BNPL Landscape

**Embedded Finance Overview:** According to researchers, placing financial offerings into areas outside banking makes banking functions component parts of other goods. Ride-sharing apps that let you pay directly in the app and e-commerce sites that can give you instant financing are included in embedded finance. He adds (2025) that "future innovations will make sure the financial system is always accessible in apps, platforms and services we regularly access". People worldwide are noticing that the technology is changing fast: Dealroom and ABN AMRO Ventures say that embedded finance could reach a market size of $7.2 trillion by 2030. To hold their place, traditional banks are now teaming up with fintechs or offering their own embedded products.

BNPL is a popular service within the world of embedded finance. Industry and academic studies notice how much BNPL has grown very fast. Malkoochi (2025) states that the BNPL market turned over $5.01 billion in 2021 and is expected to be worth $90.51 billion by 2029, increasing 43.8% each year on average. According to industry reports, including O'Connor's (2025), Worldpay data shows BNPL in e-commerce rose from $2.3B (in 2014) to $342B (in 2024), with estimates of $580B by 2030. As a result, BNPL is now recognized as a rapidly expanding way to pay worldwide. BNPL is especially popular with young people and the less financially prepared, because approval usually only involves light checks (Kumar & Backer, 2021). According to the CFPB (2022), more than 70% of BNPL providers use credit information and rely on screening by other companies to make decisions and they agree to most applications (approval rates up to 73% last year). While increasing the popularity of cryptocurrencies, these soft rules may be opening the door to more fraud.

Those who regulate the industry and industry bodies have taken an interest in BNPL and embedded finance. A new warning bulletin by the US OCC advised banks in the US that BNPL lending can increase the chance of fraudulent first payments. Banks should carefully assess fraud and set up controls before introducing BNPL offerings, according to the OCC. Likewise, the CFPB (2022) found that some BNPL companies check data sources and get notices that someone else opened credit in a customer's name. Many countries are starting to act: the UK's FCA has announced it will start regulating BNPL in 2026 and improve protections for consumers (O'Connor, 2025). A number of central banks and fintech regulators are reviewing BNPL and embedded services according to both anti-money laundering and consumer protection guidelines in Asia. In general, the growth of embedded finance has surpassed the rate at which risk rules and regulations have developed which has made the market prone to fraud.

Existing Fraud and Cybersecurity Research

**General Fraud Detection:** According to surveys, a lot of research has centered on well-established methods such as credit cards. Hernández Aros et al. (2024) analyzed 104 studies on fraud detection (between 2012 and 2023) and identified that most of the papers concentrated on credit card fraud detection models. Using machine learning techniques like judgment trees, these models help find any unusual activity in user transactions. The use of supervised learning is common in fraud studies, mainly because crime is rare and the data is imbalanced. Existing studies reveal that using AI or anomaly detection on transactions results in a much more accurate fraud detection than using only human rules or manual systems (Bello & Olufemi, 2024; Hernández Aros et al., 2024).

**Cybersecurity Threats:** An example of this is Vivari et al. (2022) who applied a fraud-detection approach with swarming and anomaly detection to help stop fraud in online trading. They point out that in "fintech forensics," fraud detection must deal with imbalanced data sets and the fact that attackers keep evolving. There are research projects that have explained cyberattacks in the context of finance: fraud is often supported by phishing and malware. Metibemu, in their 2025 review, uncovered that phishing was responsible for almost 35% of losses and ransomware caused 20%. That means fraud in fintech is mostly facilitated by technology problems and lies, not just by tricking people with credit schemes.

**Gap in Literature on Embedded Finance and BNPL:** A lot has been published about fraud detection, but few studies specifically discuss embedded finance or BNPL. There is little mention of these channels in most existing literature reviews (Hernández Aros et al., 2024). While a small number of practitioners have explored BNPL fraud qualitatively (as in Kumar and Backer, 2021), there are not many scientific studies about the topic. This year, Shu (2024) examined fraud in Buy Now Pay Later data by means of machine learning, proving new academic attention in the area, but such studies are still only beginning. Because of this gap, this research was performed by joining knowledge from fintech and fraud detection fields with industry reports to study how fraud in embedded finance is moving forward.

Key Fraud Vectors in Embedded Finance

Different sources name the fraud methods that appear in embedded finance and BNPL today. F5 Labs' analysis explains many of the common fraud attacks happening in BNPL services (Kumar & Backer, 2021). These include:

- **Account Takeover (ATO):** A small credit line is usually given when a new BNPL account is opened which can grow with use, as explained by Kumar and Backer (2021). Those with stolen credentials may log into an existing BNPL account, stealing the benefits of that account's credit and reliable repayment.
- **Synthetic/New Account Fraud:** People who steal or make fake identity documents may use them to open many new BNPL accounts, each with the issuing line of credit. Kumar & Backer talk about situations where criminals work with merchants to convert the credit into cash.
- **Stolen Payment Methods:**Since most payments for BNPL are charged to credit cards or bank accounts, fraudsters can easily use this system by paying their debt with information they have stolen. Kumar & Backer observe that some people use other people's credit cards for BNPL payments, resulting in problems and chargebacks for the sellers.
- **Identity Theft:** Alexander points out that combining true and false information is specifically hard for BNPL services (Alexander, 2025). As BNPL seldom needs thorough credit checks, it can more easily let slip through accounts belonging to synthetic identities (Alexander, 2025). Alloy's fraud-risk report shows that new embedded finance products are considered easy pickings for criminals who plan to target them at launch because they believe the controls are not completely secure.
- **Merchant and Referral Collusion:** Criminals and merchants can team up to make big BNPL purchases, never pay and share what they gain illegally. In Kumar & Backer (2021), the authors discuss how buy and sell transactions sometimes appear normal, but involve both parties agreeing on a coordinated fake sale.
- **Phishing and Social Engineering:**Attackers might send phishing emails or build false websites to fool users and get them to give permission for BNPL transactions or hand over their login data. Metibemu (2025) and Darwish et al. (2025) point out that phishing is still a major way that fintech systems are attacked.
- **Third-Party Breaches:** Embedded finance usually relies on several organizations (a fintech app, banks and providers). An attack at any point can endanger a large number of accounts. In 2024 ransomware attacked Evolve Bank & Trust (a fintech sponsor), exposing the personal data of customers using BNPL services from Affirm and other lenders. These cases prove that risks commonly affect multiple levels of embedded systems.

Sometimes, these banking fraud methods are combined with regular cybersecurity issues. Author Darwish and colleagues (2025) point out in their study that because malware, bots and automated tools are being used more and more, ATO risk is increasing. The fact that many BNPL transactions happen online, often via mobile apps, also exposes them to the broader set of cyber threats facing mobile banking (phishing, Trojans, API hacking).

Fraud Detection and Mitigation Technologies

**Identity Verification:** Layered security measures including MFA, looking into credit scores and spotting unusual activity are used by traditional banks to stop fraud. Many of these tools are also being introduced in embedded finance, thanks to AI.

**Behavioral and Contextual Analysis:** To stop synthetic identity and fake sign-ups, fintech companies are using improved methods to check user IDs. They state that during account opening, biometrics should be used and the "liveness" of the user should be checked as well. Some BNPL services have begun using identity databases, asking out-of-wallet questions and scanning documents with digital vision (Alloy, 2023). Using several verification factors makes it secure to confirm everyone's identity.

**Anomaly Detection and Rules Engines:** Using data, machine learning models can find unusual activity. As Malkoochi (2025) points out, having AI-based scoring reduces this type of error by as much as 60% and helps find more fraud. Similarly, the authors develop behavior patterns of traders to identify when something unusual is happening. Among the tools they use are observing device footprints, changes in how someone purchases and sudden alterations in payment methods.

BNPL companies usually use rules to look for things such as mismatched billing and shipping addresses or too wide geographical gaps. Even so, strict rules usually don't work; according to Malkoochi (2025), surveys indicate that only 32% of merchants feel rules engines spot fraud successfully. That's why using a mix of rules and ML is recommended.

**Third-Party Risk Management:** Since embedded finance relies on collaboration with APIs and other organizations, it's very important that all links are secure. Third-party risk is strongly emphasized in this industry (Alloy, 2023). In this way, banks need to ensure that partner fintech companies are following anti-money laundering rules and cyber security standards before proceeding. Certain embedded finance services (such as banking-as-a-service) are now applying continuous monitoring of what their partners do and the data shared.

**Regulatory and Compliance Tools:** BNPL providers are using tools for regulatory and compliance purposes. Lenders, according to the CFPB, check data brokers and outside companies to detect past dishonesty.

Additionally, rules in the works will require more affordability and better identity verification which will help make the system more secure.

Cybersecurity Implications

The rise of fraud in embedded finance has several implications for cybersecurity:

**Expanded Attack Surface:** Finance features in any non-bank app can be used by attackers to gain access. Likewise, social media and gaming platforms allowing in-app purchases with BNPL credit expand the type of people who can be targeted. Any errors in a software stack's setup like with APIs could open the door to financial risks. That means anyone building embedded apps has to use the same level of security as banks.

**API and Data Security:** It is API interactions that allow embedded finance to bridge the gap between computer apps and the financial system. If your APIs are not secured enough, attackers could either change transactions or take sensitive information. Those writing on security warn that APIs require regular penetration testing as they mature. Because of data privacy laws (GDPR, CCPA, etc.), fintech partners are required to properly handle personal information; failing to do so could result in both penalties from the law and losses from fraud.

**Identity and Authentication:** Weak checks of identity are a main reason for fraud in embedded finance. Cybersecurity means that using biometrics, hardware tokens and behavioral biometrics for identification becomes very important. Certain analysts believe decentralized identify (blockchain) could limit the need to handle personal data centrally.

**AI and ML in Cyber Defense:** More machines are now using AI for protecting systems from online fraud. On the other hand, attackers have methods to either misrepresent or ruin ML models (adversarial attacks). So, cybersecurity here must address the reliability of AI models. They believe that since issues like hard-to-understand findings and changes in the nature of fraud keep coming, AI models must be tuned from time to time.

**Regulatory Cybersecurity Standards:** As payments are regulated, embedded finance will also need to follow mandates such as PCI DSS and SCA. For example, the UK is setting up new rules which may increase the authentication measure for BNPL. If a third-party breach happens, the embedded products' sponsors are not always shielded from legal consequences (Alloy, 2023.)

**Incident Response Coordination:** Since several groups are responsible (the bank, the fintech platform and the merchant), responding to incidents in embedded finance is a challenge. An attack on just one part of the network may lead to more problems. The issue with Affirm/Evolve has proven this point: Evolve Bank's data affected a number of fintechs embedded with its database (Affirm, Wise, Mercury). Partners in the group should hence agree on joined or partner-based incident response guidelines.

By definition, embedded finance integrates financial safety into the larger software world. Both banks and fintechs need to strengthen their cybersecurity in e-commerce and platform development. Similarly, fraudsters can take advantage of the gaps between different technologies (for example, persuading the merchant, then carrying out a bad payment).

## III. Discussion

Using the existing literature, various fraud situations in embedded finance/BNPL can be analyzed and summarize ways to solve them. Several significant cases and ongoing trends are analyzed as well.

Fraud Scenarios and Techniques

The main types of BNPL fraud appear to be account takeover, the creation of new fake accounts and using stolen payment cards (Kumar & Backer, 2021). Cybersecurity is unique for different industrial sectors.

1. **Account Takeover (ATO):** In ATO, a criminal gets control over an existing user's buy now, pay later (BNPL) account. Attackers may fraudulently use the email or mobile app sign-in information of a user. A fraudster once inside a system may alter the way that payments are made or buy things without permission. Kumar & Backer point out that BNPL credit lines usually start low and then go up, so early acquisition is more attractive. If an attacker gains access to a customer's device or steals their SMS one-time password, they can enter the BNPL platform as that user. Based on reports from CNBC and IBM, account takeover lies at the heart of a huge portion of financial crime. X-Force Threat Index made by IBM (2025) reports that last year (2024), 30% of attacks exploited unauthorized use of accounts, largely directed at consumer finance services. This means that the companies providing BNPL must add extra customer authentication using devices and artificial intelligence (Bello & Olufemi, 2024). Without these, a compromised account's credentials (usually from somewhere else) can quickly be connected to embedded finance accounts.
2. **New Account / Synthetic Fraud:** The new account / synthetic fraud method finds fraudsters opening BNPL accounts in others' names to use their "easy credit" options. Since you can use BNPL without much verification, crooks can easily set up and abuse numerous accounts. Kumar & Backer (2021) mention that criminals who use pilfered driver's license or utility bill samples can both open accounts and quickly acquire goods. In his study, Malkoochi (2025) points out that synthetic identity fraud has soared in BNPL, as crooks use

both real and fake details to sneak past KYC that isn't very effective. Defending companies from this fraud involves confirming identity with document scanning and AI, checking for liveness and screening data against databases that list known fraud cases. A number of fintechs use fingerprinting devices and location tracking during onboarding to notice suspicious activity (Alloy, 2023). Yet, if crooks work with true identity theft, it is hard to identify them as fake users. Regulators believe that the large number of BNPL approvals can make synthetic fraud worse (e.g. >70%, CFPB, 2022). Therefore, the industry is considering offering similar watchlists for different services, but privacy laws might create problems.

3. **Stolen Payment Method Abuse:** BNPL often asks customers to give a payment method to pay off their purchases. They do this by using someone else's credit card information to settle their BNPL loans. Kumar & Backer explain in 2021 that criminals obtain goods using BNPL credit, but settle the fees by inputting someone else's credit card. When there's fraud, the BNPL lender covers the resulting costs and chargebacks. Since credit card numbers come from such places as breaches or the dark web, this type of attack involves payment fraud more widely. Fraud detection and credit card fraud detection are often the same – using 3D Secure and CVV checks helps prevent them. Some BNPL firms now use 3D Secure to protect themselves against fraud (as described by Kumar & Backer, 2021). Experts need to match each BNPL transaction to known shady card lists and closely watch accounts that share the same payment information for signs of abuse.

4. **Third-Party and Supply-Chain Fraud:** Since embedded finance uses many partnerships, it is especially vulnerable to third-party and supply-chain fraud. For example, fraud may be carried out by someone in the chain such as a merchant or software vendor. A merchant, knowing that a BNPL order is fake, could declare it had not been delivered so as to get a refund and keep the purchase money for themselves. A developer can include a weakness in the design of the BNPL API. The example of Evolve Bank illustrates that after a breach at its fintech infrastructure supplier (ransomware attack at the bank), not just Evolve account information was exposed but also personal data at fintech and buy-now-pay-later (BNPL) partners, including Affirm, Wise and Shopify. This means that when looking at cybersecurity for embedded finance, both the app and all its related parts are responsible. A company should always get third-party audits, stick to breach disclosure strategies and separate its data into separate areas.

5. **Emerging Tactics:** As security mechanisms become stronger, fraud creators find new ways to commit crimes. Analysts say there are now more cases of customers falsely reporting BNPL transactions, customers exploiting loyalty deals and using cryptocurrency to site illegal financial activity. Some say that fake calls using deepfake audio have been used to validate purchases by imitating someone's voice, but there aren't many solid reports yet. The report shows a rise in digital KYC being circumvented by identity spoofing powered by AI. Generally, fraud in embedded finance evolves much like fraud in other areas, rapidly moving between social media scams and BNPL and fintech.

Defensive Strategies and Technologies

What methods do embedded finance service providers use or plan, given the risks in the sector? According to the literature, censorship must be approached in multiple ways.

1. **AI and Machine Learning:** Several contributors attribute AI's importance. Malkoochi (2025) noted that companies using neural networks to detect fraud achieved better accuracy (improved from 67% to 89%) than those using traditional ways. In addition, according to Bello & Olufemi (2024), catching new types of attacks relies largely on unsupervised learning (anomaly detection). Companies using embedded finance are more likely to measure risk with ML tools by looking at transaction amounts, details about devices, locations and earlier user experience. The data used in these models can detect noticeable variance in what the user usually does (e.g. unusual international transactions, use of different devices). The difficulties arise because false positives can occur and because labeled fraud data is needed. The results indicate that by sharing anonymized information about fraud with other platforms, models could be trained more efficiently; yet, this approach is blocked by competition and data privacy.

2. **Risk-Based Authentication:** The amount of authentication required is determined by how risky a transaction seems to the BNPL app. Routine, little purchases don't need additional proof, but if you buy an expensive item or the pattern stands out, the platform might check you more carefully using one-time codes or your biometrics. This method, MFA with risk control, is proposed by Kumar & Backer (2021) and also supported by industry. ==========

3. **Data Analytics and Monitoring:** Providers regularly search for suspicious patterns in huge quantities of data. With data from payment sources, real-time analytics platforms can find and report clusters of unusual transactions. If a lot of BNPL approvals come from different accounts using the same email or IP address, it's likely a sign of a bot attack. Metibemu points out that digital banks rely on dashboards and designated limits, applying guidance from Basel III to estimate how much risk their fraud exposure represents. At times, companies rely on fraud simulation "red teams" to assess and exploit their system's vulnerabilities.

4. **Stronger Identity Verification:** Many BNPL platforms have made identity verification tougher. Today,ID authenticators also use government records, process live selfies for deepfake analysis and scan signals

from your phone to confirm you. The Financial Data Exchange (FDX) supports open banking APIs for KYC which permit verifying accounts without sharing confidential information. They point out that this helps verify in real time that the applicant has access to the bank or card account provided, restricting another approach to synthetic fraud.

5. **Regulatory Compliance and Cooperation:** Meeting regulations will help protect from some dangers. The OCC (2023) bulletin tells banks that they should create fraud risk programs focused on BNPL and include response plans for incidents. So, BNPL companies are expected to describe how they manage fraud detection and management—much like credit card issuers are required to do. Authorities in other markets are also delivering similar directions. So, due to Europe's PSD2 Strong Customer Authentication (SCA), eventually customers buying things with BNPL might need to confirm their identity using two credentials (possibly provided by a third party).

6. **Customer Education and Support:** Just as in normal banking, users must be taught about phishing and scams. Part of this approach is that users can quickly lock their accounts and report transactions that look suspicious. Now, some BNPL apps remind users when their spending habits change, so they can confirm the charges. Such UI protections are not fail-safe, but they still provide more security.

On the whole, players in the embedded finance industry are using fraud prevention solutions from banks, but they need to keep the user experience simple. The key challenge comes from the difference between making something easy to use and secure.

Case Studies and Examples

Some real examples of these have been reported to help focus the discussion.

1. **Affirm/Evolve Breach (USA, 2024):** During mid-2024, hackers used ransomware to target Evolve Bank & Trust which served Affirm and other fintechs. Therefore, users of Affirm Cards could see their personal information at risk such as names, SSNs and emails. Also, Wise and Mercury (business bank), informed their customers about leaked data from Evolve. It can be seen here that security threats from third parties can affect data that comes from embedded finance. It highlights that organizations should fully encrypt their information, control who gets in and create backup plans.

2. **U.S. BNPL Growth and Fraud:** Authorities in the U.S. have explained that BNPL customers face issues for different problems, including reports of fraud. The CFPB reported in 2022 that more people were contacting the agency to say they didn't open the BNPL accounts found on their credit reports. There are no public figures on losses yet, but the retail sector's sources claim BNPL fraud is still quite small but experiencing the fastest rate of change. It was reported by Dark Reading last year (2024) that as more people shopped online, fraudsters concentrated on BNPL, so cybersecurity had to upgrade (Dark Reading, 2024).

3. **UK BNPL Statutory Changes (2025+):** In 2025, the UK decided that from 2026, BNPL would follow regulations under consumer credit laws (FCA). Some believe that BNPL has been able to function with very little oversight, giving it a format like the wild west, in the FCA's (2025). While not a fraud case, the government is, in part, reacting to the regular fraud and debt issues happening in the BNPL world. According to UK Finance, there was a 12% rise in UK retail fraud (including APP scams) last year and fraud levels in e-commerce, where BNPL is often used, were very high. Therefore, those who provide health services are required to increase their fraud protections or be open to investigation.

4. **India's UPI and Payment Apps:** UPI and payment apps in India did not start as BNPL, but their popularity shows how huge embedded finance can be. As adoption rose, fraud also grew: in 2021-22, experts reported thousands of fraud attempts through UPI apps each day. Zeta says researchers point to methods including QR-code spoofing and social engineering. It is clear that cybercriminals never stop following the lead of financial markets. These findings are useful for BNPL companies that wish to operate in countries such as India and China: using several layers of authentication such as the PIN and phone verification used by UPI in India, is important.

As embedded finance expands around the world, fraud appears everywhere and is made possible by both electronic and human weaknesses. They make clear that different sectors are included in embedded finance, so actions must be carefully coordinated.

## IV. Conclusion

Embedded finance and BNPL are having a major impact on how financial services are provided, while also opening new security risks for companies. All the literature and reports considered clearly illustrate: criminals are manipulating well-known scams (identity theft, ATO, fraudulent payments) using what's happening now (Kumar & Backer, 2021; Alexander, 2025; Malkoochi, 2025). There are many serious cybersecurity concerns as a result.

- **Expanded Threat Landscape:** More apps now present financial risk because the landscape has grown. Social networks, ecommerce sites and service platforms can now be used by scammers to directly steal people's finances. As a result, security teams working outside of banking should pay attention to financial fraud.
- **Need for Advanced Tools:** Advanced technology is required since standard manual and fundamental forms of fraud control do not work anymore. Research (Bello & Olufemi, 2024; Darwish et al., 2025) and skilled experience (Malkoochi, 2025) demonstrate that real-time analysis and AI-supported models find patterns across different kinds of data. Still, this leads to problems related to understanding the model and privacy.
- **Regulatory Evolution:** Governments everywhere are adapting to new Real Estate developments. There will now be new rules for authentication and determining who is liable. The regulation of the BNPL field will soon become much stricter (OCC, 2023; FCA, 2025). Therefore, any embedded finance service must assume that compliance will involve considering fraud risk management first.
- **Collaborative Defense:** Because several actors are linked in embedded finance fraud (such as banks, fintechs and merchants), collaboration in fighting fraud is required. Collaborating on information about risks and agreeing on guidelines can boost the safety of the entire ecosystem.

With the sector set to be very large by 2030, researchers and experts will need to treat cybersecurity here as a major concern. It will be important for future work to examine methods for spotting fraud in BNBL data, observe user actions in these situations and invent new systems to protect user identities. Fintech organizations should make continuous monitoring, training about fraud awareness and effective dealing with incidents their top priorities.

It is clear that security must still improve for the advantages of embedded finance and BNPL to last. If stakeholders combine knowledge from books and experience from their jobs, they can find solutions for the upcoming issues with fraud. With financial services everywhere, consumers and institutions will be best protected by maintaining vigilance, using the right tech and cooperating.

## References


[1]. Alexander, N., 2025. *BNPL fraud a growing threat to user experience* [Industry article]. Bobsguide. Available at: https://www.bobsguide.com [Accessed 18 Jun. 2025].

[2]. Alloy, 2023. *Embedded finance: Navigating risks and seizing opportunities* [White paper]. Alloy. Available at: https://use.alloy.co/embedded-finance-whitepaper [Accessed 18 Jun. 2025].

[3]. Alloy, 2024. Seguin, S. (ed.) *What fraud risks do sponsor banks face in the embedded finance ecosystem?* Alloy Blog. Available at: https://www.alloy.com [Accessed 18 Jun. 2025].

[4]. Bello, O. and Olufemi, K., 2024. Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges and opportunities. *CSITR Journal*, 5(6), Article 1252. https://doi.org/10.51594/csitrj.v5i6.1252.

[5]. Bin Hendi, T., 2025. Why embedded finance is a disruptive force financial institutions can't ignore. *World Economic Forum*, 8 April. Available at: https://www.weforum.org [Accessed 18 Jun. 2025].

[6]. CFPB (Consumer Financial Protection Bureau), 2022. *Buy now, pay later: Market trends and consumer impacts* [Report]. U.S. Consumer Financial Protection Bureau. Available at: https://files.consumerfinance.gov [Accessed 18 Jun. 2025].

[7]. Darwish, S.M., Salama, A.I. and Elzoghabi, A.A., 2025. Intelligent approach to detecting online fraudulent trading with solution for imbalanced data in fintech forensics. *Scientific Reports*, 15, Article 17983. https://doi.org/10.1038/s41598-025-01223-8.

[8]. Hernández Aros, L., Bustamante Molano, L.X., Gutierrez-Portela, F., Moreno Hernandez, J.J. and Rodríguez Barrero, M.S., 2024. Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, 11, Article 1130. https://doi.org/10.1057/s41599-024-03606-0.

[9]. Kumar, A. and Backer, S., 2021. Fraud scenarios in the buy now, pay later ecosystem. *F5 Labs*, 5 August. Available at: https://www.f5.com/labs [Accessed 18 Jun. 2025].

[10]. Metibemu, O.C., 2025. Financial risk management in digital-only banks: Addressing fraud and cybersecurity threats in a cashless economy. *Asian Journal of Research in Computer Science*, 18(3), pp.434–455.

[11]. Malkoochi, R., 2025. AI-powered fraud risk scoring for Buy Now, Pay Later (BNPL) platforms. *Journal of Cybersecurity and Secure Transactions*, 1(2), pp.198–206.

[12]. O'Connor, K., 2025. BNPL expected to skyrocket to $580bn by 2030. *Payment Expert*, 14 May. Available at: https://paymentexpert.com [Accessed 18 Jun. 2025].

[13]. Office of the Comptroller of the Currency, 2023. *Retail lending: Risk management of 'Buy Now, Pay Later' lending* [Bulletin 2023-37]. U.S. Department of the Treasury, 6 December. Available at: https://occ.gov [Accessed 18 Jun. 2025].

[14]. Ping Identity, 2023. *What is embedded finance? And how identity powers it* [Blog post]. Available at: https://www.pingidentity.com [Accessed 18 Jun. 2025].

[15]. Seguin, S., 2024. What fraud risks do sponsor banks face in the embedded finance ecosystem? *Alloy Blog*, 12 June. Available at: https://www.alloy.com/blog/fraud-risk-for-banks-in-embedded-finance [Accessed 18 Jun. 2025].

[16]. Shu, J., 2024. Fraud detection models and their explanations for a Buy-Now-Pay-Later application. In: *Proceedings of the 3rd International Conference on Information Technology and Intelligent Transportation Systems (ICITITS)*, pp.1–9. IEEE. (Available via ACM Digital Library).

[17]. United States Consumer Financial Protection Bureau (CFPB), 2022. *Buy now, pay later: Market trends and consumer impacts* [Report]. U.S. Government Printing Office. Available at: https://files.consumerfinance.gov/f [Accessed 18 Jun. 2025].

[18]. Verizon, 2024. *2024 Data Breach Investigations Report*. Verizon Business. Available at: https://www.verizon.com/business/resources/reports/dbir [Accessed 18 Jun. 2025].

[19]. Williams, B., 2024. Affirm says Evolve Bank data breach also compromised some of its customers. *Malwarebytes Labs*, 3 July. Available at: https://www.malwarebytes.com [Accessed 18 Jun. 2025].