# A Simulation Game for Anti-Money Laundering (AML) Using Unity

**Long Kiu Chu and Walter Sui Leung Fung**
The Hong Kong Polytechnic University, Kowloon, Hong Kong

long-kiu.chu@connect.polyu.hk
walter.fung@polyu.edu.hk

**Abstract:** With increasing demand of anti-money laundering (AML) regulation in Fintech, AML is one of the key factors in FinTech and its regulatory technologies (RegTech). Presently, as research and education on AML focus on financial institutions and authority, the individual is vulnerable to money laundering (ML) by being money mules with lack of awareness. Therefore, this paper illustrates the design of a 2-player simulation game for AML, which integrates the game-based learning model with plots including introduction stories, player actions and ending stories. In the game, a player role-plays either a money launderer or AML specialist. Within 6 in-game months, the former needs to perform ML with a target goal while the latter needs to identify the former's actions and restrict him to achieve his goal. For actions of the money launderer, this paper integrates the criminal order with the PLI model (placement, layering and integration) to simulate the full ML circle. The criminal order provides return to the attacker if he completes it within the time limit. Each layer in the PLI model is expanded with middle processes for the methodology. The attacker uses shell companies to hide his identity and support each transaction for ML with apparently legitimate reasons. For actions of the AML specialist, this paper integrates the AML transaction monitoring with the Financial Action Task Force (FATF)'s Forty Recommendation. The defender needs to perform AML transaction monitoring with identifying suspicious financial activities based on money flow. Then, he needs to identify the actual beneficial owner of suspected companies with their share distributions. Both money flows and share distributions are visualized in data charts. Later, the defender shall report suspicious companies to the Financial Intelligence Unit (FIU), which will return the investigation result at the beginning of the next in-game month.

**Keywords:** AML, Simulation game, RegTech, FinTech, Game-based learning

## 1. Introduction

FinTech is a disruptive innovation with transforming financial services, but such disruption needs to be regulated and compiled with anti-money laundering (AML) and counterterrorist financing (CTF) laws to protect the global financial system (Duhaime, 2019). Both are regulated by RegTech to combat financial crime (Hanley-Giersch, 2019). Therefore, AML is one of the key factors in FinTech and RegTech. As existing research on AML education focuses on financial institutions and authority, it might ignore individual education for their AML awareness. The individuals might be exposed to the risk of being lured into money mules of money laundering (ML) (The Guardian, 2021).

This paper illustrates the design of a simulation game for AML to raise awareness of ML and AML through game-based learning with our simulation game. The game will be evaluated by students' feedback on the gaming for investigating the effects of knowledge delivery with the simulation game.

## 2. Literature review

### 2.1 Definition of AML and PLI model

"*AML aims to halt financial criminals from disguising illegally obtained funds as legitimate ones*" (ACAMS, n.d.). In other words, AML is to combat money laundering. ML consists of three stages: Placement, Layering, and Integration (United Nations, Office on Drugs and Crime, n.d.). Placement is to place illegally obtained income into financial institutions (ACAMS, n.d.). Layering is dividing dirty money by layers of legitimate transactions to hide the source of the dirty cash (ACAMS, n.d.). Integration is to support illegally obtained wealth with "apparent legitimacy" by re-entering the economy to disguise it as normal transactions from businesses and individuals (ACAMS, n.d.). All three stages of ML form the PLI model, which is the foundation of the ML method in this paper.

### 2.2 Financial Action Task Force Forty Recommendations

When discussing AML and CFT laws for the global financial system, it is unavoidable to introduce Financial Action Task Force (FATF) with its standardization on AML regulations and operations. Its Forty Recommendations published in 1990 is a comprehensive AML guideline for the international safeguards and governmental standards to combat financial crime (FATF, n.d.). Combining FATF Forty Recommendations with game-based learning on AML could help players stay grounded to the global standard.

### 2.3 Game-Based Learning With Simulation Game

Game-based learning (GBL) is a type of gameplay with defined learning outcomes (Shaffer, Halverson, Squire, & Gee, 2005) in behaviorism, cognitive, constructivism, humanism, and connectivism (University of Phoenix, n.d.). Plass et. al (2015) contributed to the foundations of the GBL with a model and design framework. The model is a continuous loop in general with a challenge, response, and feedback (Plass et.al, 2015). The design framework is integrated learning game design elements with four foundations: affect (i.e., constructivism), motivation (i.e., behaviorism), cognitive, and social or cultural (i.e. connectivism or humanism) (Plass et. al, 2015).

One of GBL examples in digital forms is simulation games. It serves the purpose of education to represent the player with a simulation with a focus on a mimicking real-life scenario (Kruk and Peterson, 2020) to facilitate "learning" (i.e. *acquiring or enhancing knowledge and skills*) and "simulation" (i.e. purpose to facilitate learning primarily or support learning indirectly) (Frasson and Blanchard, 2012). Although the simulation part focuses on *imitating one process by another process* for scientific purposes with typically perceiving physics elements (Hartmann, 1996), it could integrate financial and AML elements into the simulation to achieve GBL on AML.

### 2.4 Existing Business Simulation Games

As simulation games or Serious games provide individualized instructions and measure educational outcomes, they are a powerful delivering channel to achieve educational outcomes (Routledge, 2015). For business simulation games, a typical example is Harvard Business Simulations (n.d.) which integrates business concepts with realistic business scenarios to allow users to make decisions based on visualized data diagrams and charts. It provides a design direction for designing the methodology of this game.

### 2.5 Existing ML Simulation Games

The internet consists of ML simulation games. One example is the work from i-KYC (n.d.), which adopts a plot-based visual novel to educate players on ML concepts. Another example is the ML Simulator from Candlesan (n.d.), where a player shall roleplay a money launderer to launder a target amount of money with given methods each day and avoid being caught by the FBI.

### 2.6 Existing AML Simulation Games

Most of the anti-money laundering simulation games are designed for corporations.

For corporation training, Hernández Sánchez (2018) included risk management for ML in their game for organizational training purposes. Another example is True Office (True Office Learning, n.d.), which is a game-based training tool for compliance topics such as anti-money laundering.

For roleplaying with the theme of the corporation, Games4Substainability (n.d.) developed a 3D game called Anti Money Laundering, where players roleplay AML specialists to investigate the financial crime with the PLI model and provided AML-related glossary for references. Also, Anti ML Centre and PwC (2021) co-developed the AML pressure cooker, where players roleplay the Advisor of a suspicious company NaBook to identify whether it is secretly used for money laundering. During the investigation, players can access the dashboard and hint to learn the ML in gaming.

## 3. Project Methodology

### 3.1 Two Player Game Approach

As existing works specify the theme of either ML or AML, there are no AML simulation games for players to perform both ML and AML. Regarding this, the methodology adopts a two-player game approach with one player as a money launderer and another player as an AML specialist. Both players will combat each other to simulate the attack and defend during ML in a bank. The gameplay follows a generic plot with decisions to get endings based on their in-game performance.

### 3.2 Game-Based Learning With Plots

Our work is designed to link the GBL model with plots for both attacker and defender. Based on the GBL model, the game induces a challenge with introduction stories, receives responses from players, and gives them feedback with ending stories.

### *3.2.1 Challenge with introduction stories*

For introduction stories, both stories are delivered in videos to explain the identity and mission of each player. Represented in visual and audio, the stories situate the theme and background to facilitate the cognition of their role. Additionally, it integrates with the emotional representation of affection. The attacker's story is inspired by the story of the world's famous money launderer Bruce Aitken, who laundered money for the dark side of a government but realized that he broke the law later (SCMP, 2022). Like Bruce's situation, our plot mimics the situation where the attacker realizes that he will be eliminated by the government with his dirty work and must earn $1,000,000 to escape overseas with sufficient capital to maintain his living. Besides, the defender's story informs him of the duty of being an AML specialist and the consequences of failing to safeguard the bank.

### *3.2.2 Receive response from players*

After the introduction stories, players take action to respond to the game. The attacker receives dirty money from criminals privately and performs ML by the PLI model. The defender disturbs the attacker's ML activities by AML transaction monitoring and reports any companies with suspicious financial activities to the Financial Intelligence Unit (FIU). The response period consists of 6 months, where each month has 4 weeks for both players to respond. Each week, the attacker takes action first while the defender observes financial activities at the end of the week.

### *3.2.3 Give feedback to players with ending stories*

After six months of the response period, the game analyses the in-game performance of both players and gives feedback to them with a performance summary and ending stories. For the performance summary, the attacker is evaluated with the success rate of laundered money (i.e. the amount of successfully laundered money over the received dirty money) and the percentage of the laundered money to the target goal of $1,000,000. The defender is evaluated with the accuracy rate of reported companies (i.e. the number of companies reported with actual ML activities over the number of companies reported) and the success rate of ML halted (i.e. the halted amount of laundered money over the total amount of laundered money).

Based on the evaluation, both players receive an ending story respectively. Figure 1 shows that the attacker has two ending stories with whether he can achieve the target goal. Figure 2 shows that the defender has three ending stories with two criteria: the accuracy rate of reported companies is not lower than the acceptable default and whether the attacker achieves his ML goal.

| | Ending stories |
|---|---|
| Can earn the target goal $1,000,000 | Good Ending<br>(Attacker successfully escapes to overseas) |
| Cannot earn the target goal $1,000,000 | Bad Ending<br>(Attacker is caught by the government) |

**Figure 1: Ending stories for the attacker**

| | | Can Attacker achieve his money laundering goal? | |
|---|---|---|---|
| | | Yes | No |
| Is Accuracy rate lower than acceptance default? | Yes | Bad Ending<br>(The bank is fined by the government while the defender is fired by the bank) | Neutral Ending<br>(The defender protects the bank from money laundering, but the senior does not like too much unnecessary filing.) |
| | No | | Good Ending<br>(The defender protects the bank from money laundering and get a promotion) |

**Figure 2: Ending stories for the defender**

As emotional events can provide clearer, more accurate, and more long-lasting delivery (Tyng et. al, 2017) to facilitate learning, the ending stories adopt different music and content depending on the game result to raise players relevant emotions. If the player wins the game, it will adopt happy theme music and plot to emphasize the happiness of winning. If he loses the game, it will adopt sad theme music and stories to emphasize the disappointment of losing.

### *3.2.4 Intense gameplay with monthly report*

Sessions 3.2.1-3.2.3 form a general loop for the GBL model. However, if players keep playing all 24 in-game weeks to gain feedback, their attention start declining after 20 minutes (Bradbury, 2016) without a break. Therefore, we design the game by providing a monthly report to both players to send them intermediate feedback and pause the game for a break before proceeding to the next in-game month. For the attacker, the monthly report shows the estimated money flow trend of normal companies and shell companies reported by the defender to make a strategy. For the defender, it informs the defender once the attacker has attained each quarter of his target goal. Providing up-to-date information to both players can intensify the gameplay by motivating them to counter other players. If any player meets his winning goal in any in-game month, the game will end immediately by showing end game summary and ending stories.

## 3.3 Actions of the Attacker

The actions of the attacker consist of four layers, where each layer shall either keep the current action status or pass data to the next layer. The first layer is the source of dirty money, which is named as criminal order. The other three layers are the PLI model: placement, layering, and integration.

### *3.3.1 Attacker: Criminal order*

*Organised criminals use professional ML syndicates to conceal the illicit nature of funds sourced from criminal activities* (Australian Federal Police, n.d.). As the attacker is a professional money launderer in the plot, he will receive several orders from criminals to launder their dirty money. Each order rewards the attacker with a percentage of the dirty money, but it has a time limit to fulfill the ML process.

### *3.3.2 Attacker: Placement*

Placement is placing dirty money into the bank, but it is obvious for such practice because the attacker cannot provide a legitimate source for the placed money. Therefore, it needs a middle process for transforming dirty money into other forms of assets including casino tokens, cash funds, cash, gold, cryptocurrency, and foreign currency. Then, those assets will be transformed into three forms of currency including local currency, cryptocurrency, and foreign currency. Casino tokens and gold are sold to local currency while the cash and cash funds are assumed another representation of local currency. Last, those three forms of currency will be placed into the bank for the layering process later.

### *3.3.3 Attacker:Llayering*

Layering needs to use layers of transactions to hide the originality of dirty money. The attacker should not use his personal identity directly to perform transactions risking being exposed to the bank. Instead, he should own a shell company to remote control other shell companies to perform transactions for layering. Such practice allows hiding his identity during the layering. Each transaction for layering is a Transaction object including sending status, receiving status, the week the transaction occurred, and the legitimate reason for the transaction. The sending status includes the name of the sender, the sent item type, and the sent amount. The receiving status includes the name of the receiver, the received item type, and the received amount. The week of the transaction occurred is named transaction week. The legitimate reason is a transaction type for money outflows of a company including purchase, operational expense, interest expense, lending, and investment. The relationship among the attacker, shell companies, and transaction are shown in Figure 3.

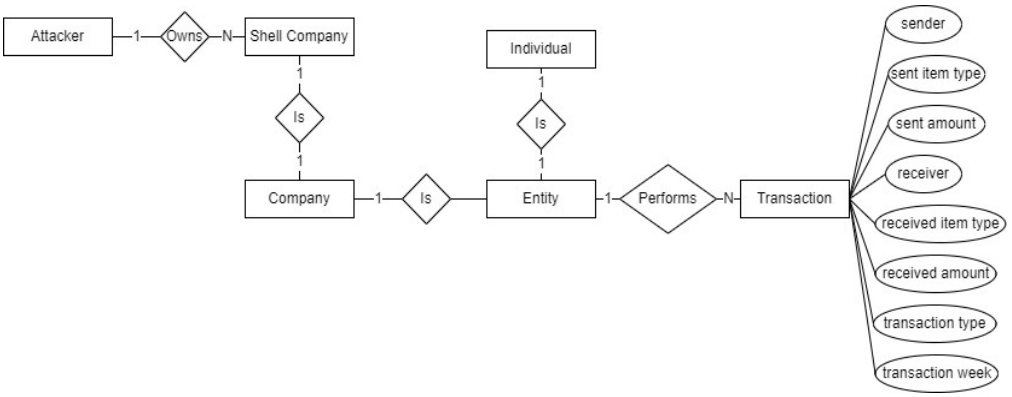


**Figure 3: Entity Relationship Diagram in the Layering layer**

To connect the placed currencies in the placement layer to this layer, we allow the attacker to spend all three types of currencies with local payments (i.e. onshore payments) and cross-border payments (i.e. offshore payments). Onshore payments are transactions using local currency and cryptocurrency while offshore payments use foreign currency and cryptocurrency. Depending on the attacker's strategy, he could keep performing a transaction after a transaction or stop processing.

### *3.3.4 Attacker: Integration*

Integration is to support dirty money with apparent legitimacy to disguise as normal transactions from companies. Those transactions are from layering transactions, but their receiver is a specific bank account for both the attacker and criminals to extract laundered money and spend it as legitimate income. Before extracting the money, those transactions are checked by the bank with AML transaction monitoring. If it is caught by the bank, the bank account of shell companies will be frozen so the attacker will lose his effort of ML with the frozen account.

### *3.3.5 Summary*

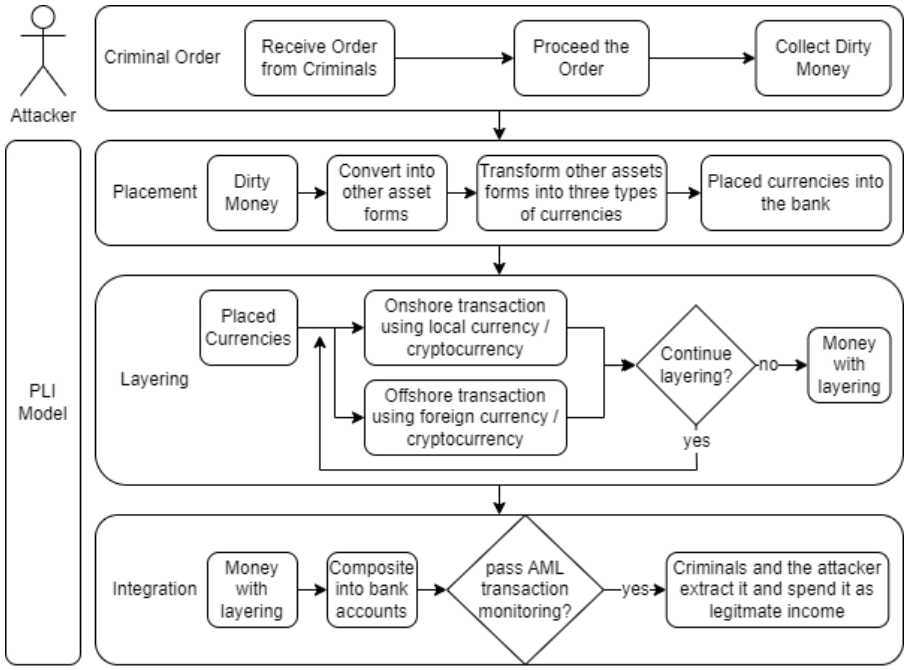


**Figure 4: Summary of the attacker's actions**

## 3.4 Actions of the Defender

The actions of the defender start from performing AML transaction monitoring to identify companies with suspicious financial activities. Then, the defender will identify the actual beneficial owner of the suspected companies by share distribution. Afterward, the defender can report all companies owned by the actual beneficial owner to the Financial Intelligence Unit (FIU) for further investigation.

### *3.4.1 Defender: AML transaction monitoring*

AML transaction monitoring is to monitor customer transactions based on customer activity, which is developed by customer information and interactions currently and historically to access the client risk (SAS, 2022). A company generates money flows from its operations. If it is a shell company for money laundering, the money flows are from ML activities, which are transactions from the attacker. To identify the shell companies among all companies, the defender observes visualized money flows in a line chart each week among all transaction types to spot suspicious financial activities with abnormal patterns.

### *3.4.2 Defender: Identify actual beneficial owner*

FATF Recommendation 10 (2012) stated that customers suspected of ML activities should be conducted with customer due diligence by identifying the actual beneficial owner with reliable and independent data sources. Once discovering any companies with suspicious financial activities, the defender should identify the actual beneficial owner by observing the share distribution, visualized by a pie chart. In our work, the actual

beneficial owner is the largest shareholder of a suspected company. If the defender is confident that the actual beneficial owner is the attacker's shell company, all companies with the particular shell company as the largest shareholder shall be reported to FIU.

### *3.4.3 Defender: Report suspicious companies to FIU*

FATF Recommendation 20 (2012) stated that financial institutions with suspects of ML should be reported to the FIU regardless. After identifying the actual beneficial owner of any suspected companies, the defender can report these companies to the official institution FIU for further investigation. *The FIUs function as an intermediary between the private entities, subject to AML/CFT obligations, and law enforcement agencies* (Council of Europe, n.d.). During the investigation, banks may freeze banks accounts of reported companies with suspected ML (Deacons, 2020). In the game, assume the FIU can give investigation results of reported companies to the bank in a month. If the reported companies are one of the attacker's shell companies, the bank will keep freezing the bank account. Otherwise, it will unfreeze innocent bank accounts. To prevent abuse of reporting to achieve guaranteed winning for the defender, the minimum accuracy of reporting has an acceptable default of 70%.

### *3.4.4 Summary*

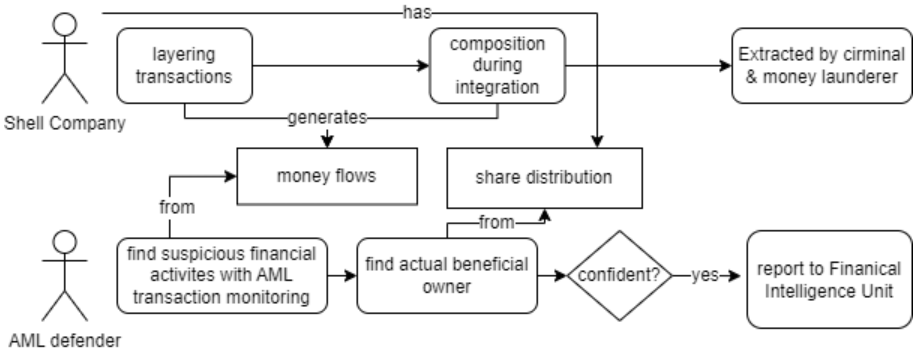


**Figure 5: Summary of the defender's actions**

## 4. Implementation

### 4.1 Game Flow

If a room is matched with two players, the room host can start the game. At the beginning of the game, players select their roles and watch associated introduction stories. Both players perform actions to give a response. For the attacker, it is criminal order and the PLI model. For the defender, it is the AML transaction monitoring, identifying the actual beneficial owners and reporting suspicious companies, where the share distribution and normal companies' money flow are stored in an embedded CSV file. After the game ends, the game gives feedback to players with an evaluation summary and ending stories. The game flow is shown in Figure 6.

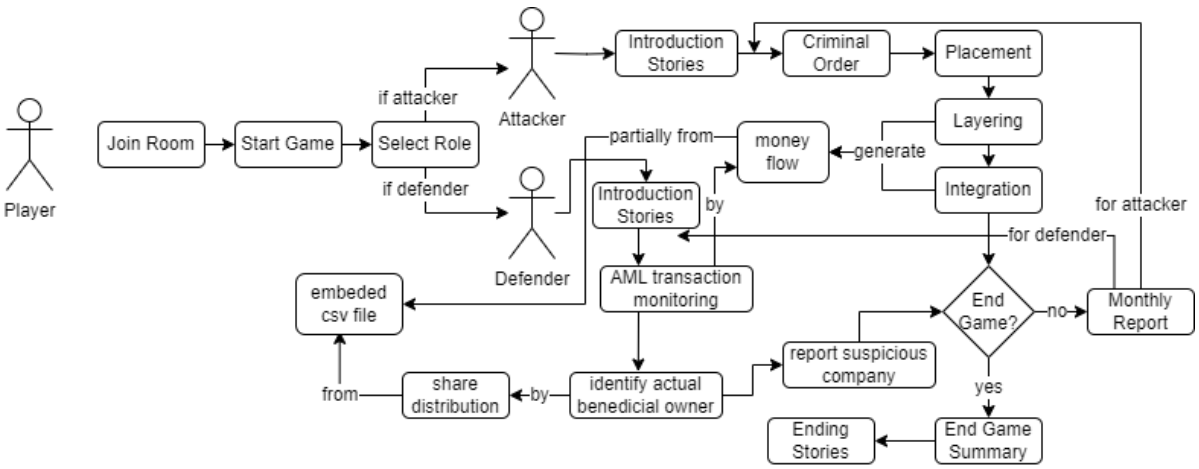


**Figure 6: Graphical Expression in the game flow**

### 4.2 Networking for two Player Game

As our work is implemented with Unity, the networking among players adopts the Photon Unity 3D Networking (PUN) framework from Photon (n.d.), which is a peer-to-peer (P2P) networking solution. This framework is hosted by Pun's cloud services for room matching and data transmission. Each player is a peer who holds all components and enables partial components based on the in-game scenario. Figure 7 shows the networking architecture for the game.


**Figure 7: Networking architecture diagram for the game**

### 4.3 Role Selection

As each peer holds all components, when players select to be either attacker or defender, a role selection mechanism (see Figure 8) restricts access to them to prevent either the case that one player selects two roles or the case that one role is selected by two players.

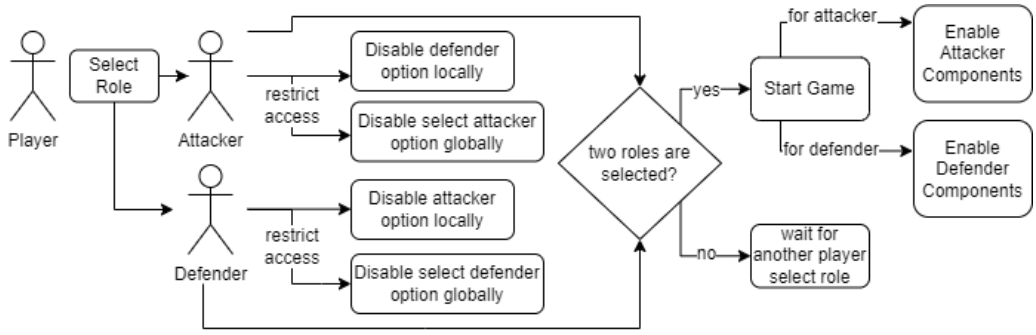


**Figure 8: Detailed Flow of role selection**

## 5. Evaluation

The effectiveness of our AML simulation game is evaluated by comparing the pre-surveys and post-surveys with 50 students invited in total. Both surveys are conducted to measure their overall score in awareness of ML and AML. Compared to the pre-surveys, the results of post-surveys showed an increase in scores of awareness in both ML and anti-money laundering. In other words, students responded that they will be more aware of the ML process (i.e. placement, layering, and integration) and AML concepts like transaction monitoring and FATF in their daily life. Besides, students reported that they had heard of ML and AML but had not heard of FATF and its Forty Recommendations, showing the need of integrating official institutions such as FIU and FATF in the education of AML to the students. As the students reported that they received useful information from the plots and in-game actions, the design of GBL with plots was positively received by the students. However, it is reported that it is too time-consuming to spend at least an hour to complete the gaming with 24 in-game weeks. Another suggestion from the students is adding a glossary of terms for explaining keywords used in the plots and in-game actions. Therefore, the results of surveys suggest that the game can educate users with concepts of ML and AML including the ML circle, and overview of regulation institutions of AML, but it can be further improved by adjusting the time length of gaming and adding a glossary of terms.

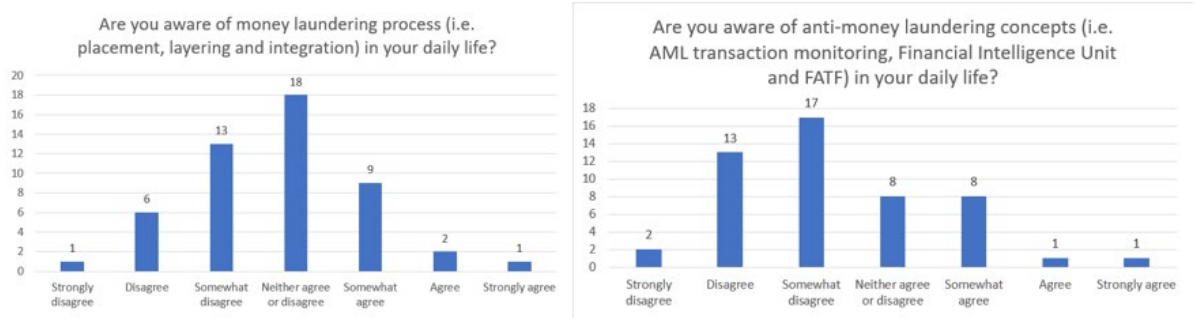


**Figure 9: Results for pre-survey on the awareness in ML and AML**

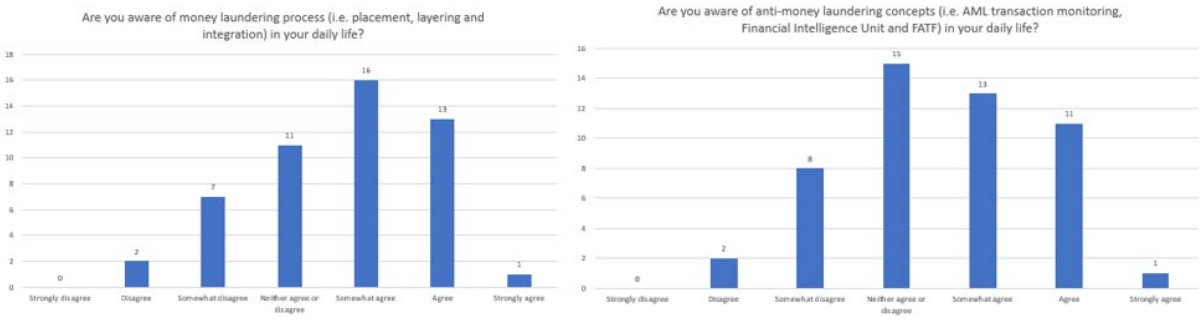


**Figure 10: Results for post-survey on the awareness in ML and AML**

## 6. Conclusion

This paper illustrates the design of a simulation game for AML implemented by Unity. The objective of the design is to educate individuals about ML and AML knowledge to raise awareness in daily life to reduce the risk of being a money mule. The game consists of two roles: the money launderer as the attacker and the AML specialist as the defender. Both players combat each other to attack and defend during ML in a bank. The game delivers game-based learning with plots including introduction stories, in-game actions, and ending stories. The introduction stories illustrate the background and mission of each player. The attacker needs to earn a target amount of $1,000,000 with ML for his saving in migrating overseas to escape the government. The defender needs to safeguard the bank from ML for his job. The in-game actions have 24 in-game weeks for both players to counter other players' actions. The attacker will receive dirty money from criminals and perform ML using the PLI model (i.e. placement, layering, and integration). He will use a shell company to remote control other shell companies to perform transactions to disguise the ML as business operations and integrate the money into the bank. The defender will perform AML transaction monitoring to identify companies with suspicious financial activities. Then, based on FATF Recommendation 10, the defender will identify the actual beneficial owner of suspected companies with share distribution. Based on FATF Recommendation 20, he will report all companies owned by the actual beneficial owner to the FIU for further investigation and freeze their accounts before receiving the investigation result. If the investigation result validates the report, the bank will keep freezing the bank accounts to halt money laundering. Otherwise, it will unfreeze the bank accounts. Before the ending stories, the game will show an end-game summary to evaluate players' performance. Then, it will play ending stories based on the player's performance to give feedback. To intensify the gameplay, there is a monthly report at the beginning of each month to provide players with up-to-date information to make more valid decisions.

This simulation game is developed by Unity. The money flow of normal companies and the share distribution of all companies are stored in an embedded CSV file. The networking adopts the Photon Unity Network #D framework for its peer-to-peer solutions, which are hosted by Photon Cloud services. As a P2P game, each peer holds all components and enables part of them based on gaming scenarios. Therefore, a role selection mechanism is discussed to prevent either the case that one player selects more than one role or the case that one role is selected by more than one player.

The evaluation of this paper is conducted by comparing pre-surveys and post-surveys of 50 students. The results of surveys suggest that the game can educate users with concepts of ML and AML including the ML

circle, and overview of regulation institutions of AML, but it can be further improved by adjusting the time length of gaming and adding a glossary of terms.

The limitations of this paper's work are acknowledged.

- AML of the banking industry is confidential. Our work has no access to the most detailed information and solution of current industrial practice.
- Methods of ML should not be limited to companies and considered using money mules.
- As ML could vary based on the money launderer's practice, the design tries to provide a more generic approach. Details like transaction type of companies are assets forms in placement might not be the same as the real-life scenario.
- We did not have money flows data from companies to simulate the financial activities of normal companies without money laundering.
- The attacker could memorize all the money flows of normal companies and pretend normal companies with the memorized money flows. In real scenarios, the attacker needs to figure out the normal pattern of money flow by themselves when attempting to use shell companies for money laundering. Data for the attacker to guess such a normal pattern is not provided in this work.
- Evaluations of the end game are more focused on the defender with providing the confirmed reports of the attacker's ML acts. However, the reason why the ML activities of the attacker are caught by the defender is not answered by both parties.

## References

ACAMS (n.d.). AML Glossary of Terms | ACAMS Trending Topics. Retrieved April 27, 2023, from https://www.acams.org/en/resources/aml-glossary-of-terms#b-439f2d68

ACAMS (2012-2016). Study Guide of CAMS Certification Exam.

Anti ML Centre (2021). Anti ML Game. Retrieved April 28, 2023, from https://amlc.eu/anti-money-laundering-game/

Australian Federal Police (n.d.). ML | Australian Federal Police. Retrieved June 10, 2023, from https://www.afp.gov.au/what-we-do/crime-types/proceeds-crime/money-laundering

Bradbury, N. A. (2016). Attention span during lectures: 8 seconds, 10 minutes, or more?. Advances in physiology education.

Candlesan (n.d.). ML Simulator | idjam.com |Ludum dare game jam. Retrieved April 28, 2023, from https://ldjam.com/events/ludum-dare/40/money-laundering-simulator

Council of Europe (n.d.). Financial Intelligence Units - Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. Retrieved April 30, 2023, from https://www.coe.int/en/web/moneyval/implementation/fiu

Deacons (2020). The freezing of customer bank accounts for ML reasons - Deacons - Law Firm - Hong Kong. Retrieved June 11, 2023, from https://www.deacons.com/2020/09/16/the-freezing-of-customer-bank-accounts-for-money-laundering-reasons/

Duhaime, C. (2019). The Role of Anti-Money Laundering Law and Compliance in FinTech. In J., Barberis, D. W., Arner, & R. P., Buckley (Ed.), The REGTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation. (pp. 190-194). John Wiley & Sons, Incorporated.

Financial Action Task Force (n.d.). FATF Recommendations. Retrieved April 27, 2023, from https://www.fatf-gafi.org/en/topics/fatf-recommendations.html

Frasson, C., Blanchard, E.G. (2012). Simulation-Based Learning. In: Seel, N.M. (eds) Encyclopedia of the Sciences of Learning. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-1428-6_129

Games4Sustainability (n.d.). Anti Money Laundering. Retrieved April 28, 2023, from https://games4sustainability.org/gamepedia/anti-money-laundering/

Hanley-Giersch, J. (2019). RegTech and Financial Crime Prevention. In J., Barberis, D. W., Arner, & R. P., Buckley (Ed.), The REGTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation. (pp. 20-25). John Wiley & Sons, Incorporated.

Hartmann, S. (1996). The World as a Process. In: Hegselmann, R., Mueller, U., Troitzsch, K.G. (eds) Modelling and Simulation in the Social Sciences from the Philosophy of Science Point of View. Theory and Decision Library, vol 23. Springer, Dordrecht. https://doi.org/10.1007/978-94-015-8686-3_5

Harvard Business Publishing Education (n.d.). Simulations | Harvard Business Publishing Education. Retrieved April 29, 2023, from https://hbsp.harvard.edu/simulations/

Hernández Sánchez, M. (2018). Model of a game-based virtual learning environment to support training processes in organizations. Escuela de Sistemas.

i-KYC (n.d.). The i-KYC ML Challenge. Retrieved April 28, 2023, from https://i-kyc.com/kyc-academy/money-laundering-game/story_html5.html

Kruk, M., & Peterson, M. (2020). New technological applications for foreign and second language learning and teaching (M. Kruk & M. Peterson, Eds.). Hershey, PA: Information Science Reference.

Photon (n.d.). Photon Unity 3D Networking Framework SDKs and Game Backend | Photon Engine. Retrieved April 30, 2023, from https://www.photonengine.com/en/PUN

Plass, J. L., Homer, B. D., & Kinzer, C. K. (2015). Foundations of Game-Based Learning. Educational Psychologist, 50(4), 258–283. https://doi.org/10.1080/00461520.2015.1122533

Routledge, H. (2015). Why Games Are Good for Business: How to Leverage the Power of Serious Games, Gamification and Simulations. Palgrave Macmillan UK.

SAS (2022). What is Transaction Monitoring in AML | SAS UK. Retrieved June 11, 2023, from https://www.sas.com/en_gb/insights/articles/risk-fraud/what-is-transaction-monitoring-in-aml.html

Shaffer, D. W., Squire, K. R., Halverson, R., & Gee, J. P. (2005). Video Games and the Future of Learning. Phi Delta Kappan, 87(2), 104–111. https://doi.org/10.1177/003172170508700205

South China Morning Post (SCMP) (n.d.). Drugs, cash and the CIA: international money launderer Bruce Aitken worked for the world's shadiest characters, revealed in his book Mr Clean. Retrieved June 10, 2023, from https://www.scmp.com/magazines/post-magazine/books/article/3178504/drugs-cash-and-cia-international-money-launderer

The Guardian (2021). Money mules: how young people are lured into laundering cash. Retrieved April 30, 2023, from https://www.theguardian.com/money/2021/oct/04/money-mules-laundering-cash-students-funds-bank-accounts

True Office Learning (n.d.). Best Online Compliance Training Software | True Office Learning. Retrieved June 11, 2023, from https://www.trueofficelearning.com/

Tyng, C. M., Amin, H. U., Saad, M. N., & Malik, A. S. (2017). The influences of emotion on learning and memory. Frontiers in psychology, 1454.

United Nations, Office on Drugs and Crime (n.d.). Overview in Money-laundering. Retrieved April 25, 2023, from https://www.unodc.org/unodc/en/money-laundering/overview.html

University of Phoenix (n.d.). 5 educational learning theories and how to apply them. Retrieved June 10, 2023, from https://www.phoenix.edu/blog/educational-learning-theories.html