ABE EBA
EURO BANKING ASSOCIATION

EBA FRAUD TAXONOMY

Joint approach to payment-related fraud type categorisation developed by the Euro Banking Association

Version 4.0

Classification: Public

7 June 2023

ABE EBA
EURO BANKING ASSOCIATION

1. Introduction to the EBA Fraud Taxonomy

Background

Stepping up pan-European co-operation to fight and prevent payment fraud has become a key priority among fraud experts in the growing real-time payments ecosystem. The Euro Banking Association (EBA) created the Expert Group on Payment Fraud-related Topics (EGPF) in February 2020 to work towards a collaborative approach to fraud-combatting in the pan-European payments industry. The objectives of the EGPF are to analyse minimum requirements for enabling a pan-European fraud intelligence approach and to define what fraud information and data could be exchanged as part of this approach. To facilitate the work on these matters, the EGPF also looked into the development of a common vocabulary in relation to payment fraud-related topics, to serve in a pan-European context.

When considering the best way forward to structure the data and intelligence that should ideally be shared to effectively detect and prevent payment fraud, the EGPF concluded that the fraud type was the most important variable driving the need for specific data input. Since no uniform set of definitions of fraud types had previously been agreed at a pan-European level, the EGPF determined to develop, in a first step, a joint approach to fraud type categorisation.

Structure of the taxonomy

The present EBA Fraud Taxonomy (joint approach to fraud type categorisation) focuses on identifying the following elements relevant to a fraudulent action: **initiator** (who), **method** (how), **modus** (what) and **labels/tags**. With these elements, it offers a standardised way to identify *who* initiated the payment transaction affected by the fraud, *how* the fraudster first contacted the victim and *what* trick the fraudster used to get hold of the victim's money or credentials. By providing labels or tags, the taxonomy additionally allows payment service providers (PSPs)s to enrich the case with additional categorisation information on a voluntary basis.

This fraud taxonomy has been designed to meet the following objectives:

- It applies to both payment fraud and card fraud.
- It creates a common vocabulary regarding fraud in the area of payments. The taxonomy builds on the work done by fraud experts around the globe by relying on definitions from authoritative and publicly available sources, wherever possible.
- It reduces the risk of overlap in the identification of fraud types and, consequently, increases the accuracy of statistics used to identify fraud trends.
- It separates the contact methods ("how") used by fraudsters from the actual tricks they apply ("what"), which supports PSPs in developing effective fraud prevention campaigns for their customers.

- It is aligned with the European Banking Authority (EBA) Guidelines on Fraud Reporting under PSD2, which have already been implemented by PSPs across Europe.
- The taxonomy is available to any interested party.

Publication history

To make sure that the EBA Fraud Taxonomy remains in line with the needs of fraud experts in a fast-changing environment, it is subject to an annual review and updating process, which is launched in October of each calendar year. The timeline governing the change cycle foresees the release of an updated version of the EBA Fraud Taxonomy normally in June of each year, so that users are provided with a six-month lead time for implementation effective on 1 January of the next year. For details on the annual change cycle, please refer to chapter 11 'Review and updating process'.

- The EBA released version 2.0 of the EBA Fraud Taxonomy in July 2021 to the financial institutions in the Association's membership for a first try-out phase with the aim to gather practical experience in deploying a uniform taxonomy at pan-European level.
- The first round of the annual review and updating process led to the release of version 3.0 of the EBA Fraud Taxonomy in June 2022.
- The EBA released version 3.1 of the taxonomy as a public document under an updated usage rights regime in October 2022, containing changes to the introduction (only) of the taxonomy to bring clarity on the usage rights ahead of 1 January 2023, when version 3.1 came into effect.
- In June 2023, the EBA released version 4.0 of the taxonomy which will come into effect on 1 January 2024. An overview of the changes introduced into version 4.0 of the EBA Fraud Taxonomy compared to the version 3.1 is set out in the Annex of this document.

Usage rights

Use of the EBA Fraud Taxonomy further entails:

- acknowledgement of the review and updating process of the EBA Fraud Taxonomy, and acknowledgement of the expectation that updated versions should be implemented by users effective on 1 January following the completion of an annual review cycle, save in case of emergency updates which may require implementation on another date; and
- adherence to the objective to create a common vocabulary for fraud types at a pan-European level without limitations on the type of payment instrument.

2. EBA Fraud Taxonomy: version history

Version 1.0	8 October 2020
Version 2.0	12 July 2021
Version 3.0	28 April 2022
Version 3.1	27 October 2022
Version 4.0	7 June 2023

ABE EBA
EURO BANKING ASSOCIATION

3. Contents

4. Dimensions to be considered in a fraud scenario

It is important to delineate the fraud type against other dimensions that are also relevant but not covered by the fraud type. The below overview shows how the fraud type fits in with other relevant dimensions:

Fraud	External fraud	Internal fraud

Victim	Bank	Bank customer

Product	Cards (incl. debit / credit)	Credit transfers (e.g. SEPA)	Direct debits (e.g. SEPA)	CNP / CP
	Investment / securities & markets	Unauthorised transaction	Lending (non-card lending)	

Who	Fraud types
How	
What	
Label	

Channel	Mobile bank app	Tablet bank app	Online	eBanking browser
	ATM	Branch	Point of sale	Third-party channel

Covered by channel & product?	
Retail	Commercial
Domestic	Cross-border

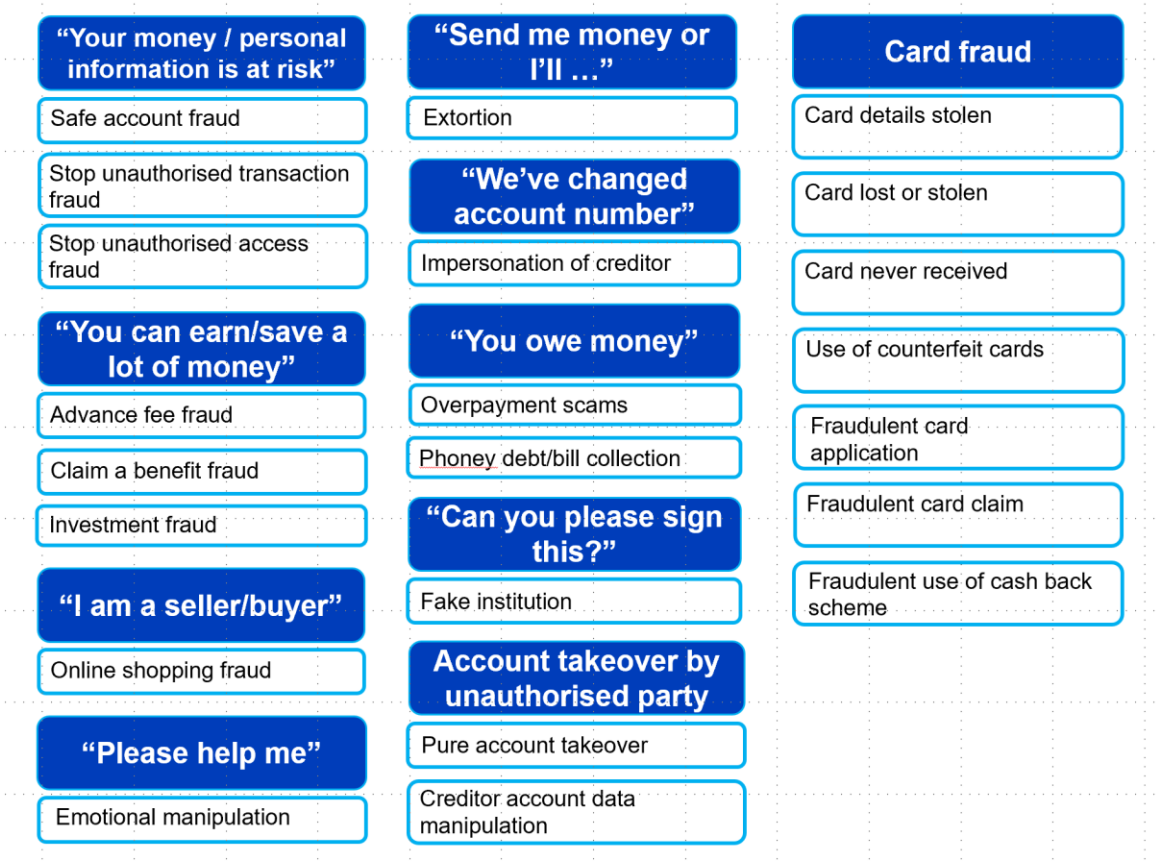
5. Description of fraud type dimensions: initiator, method, modus, labels/tags

The EBA Fraud Taxonomy focuses on identifying the following elements relevant to a fraudulent action:

The EBA Fraud Taxonomy offers a standardised way to identify *who* initiated the payment transaction affected by the fraud, *how* the fraudster first contacted the victim and *what* trick the fraudster used to get hold of the victim's money or credentials. These elements allow to describe any fraudulent event in a very brief and precise manner:

- **Initiator (who):** describes who initiates the payment transaction affected by the fraud, i.e. the customer or the fraudster. The initiator section includes 'first party' as an optional element relevant, primarily, to card fraud.
- **Method (how):** describes the attack vector and specifies the first point of contact between the fraudster and the victim or the point of compromise.
- **Modus (what):** describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction. These actions are clustered within high-level classifications reflecting the strategic approach deployed by the fraudster. For each modus, a definition is provided based on an authoritative and publicly available source, wherever possible.
- **Labels/tags (PSP individual):** to ensure ease of use and maximum flexibility, the EBA Fraud Taxonomy provides the possibility to enrich the case with additional categorisation information on a voluntary basis using labels or tags. The labels/tags listed in the taxonomy are suggestions and not meant to be exhaustive. Individual PSPs remain free to choose labels/tags for specific fraud scenarios as they deem fit, for example to align with internal reporting requirements. For each label/tag, a definition is provided based on an authoritative and publicly available source, wherever possible.

Figure 1: High-level classifications reflecting the strategic approach deployed by the fraudster and related actions (modi)*



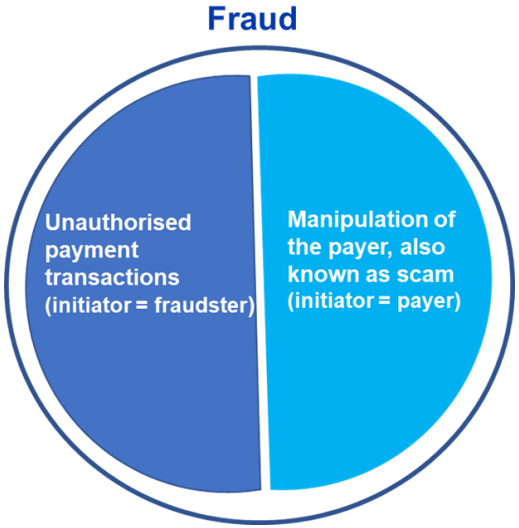
*For details, please refer to chapter 9 'Modus (what)'

6. Definition of fraud

Fraud is defined as follows:

- "Unauthorised payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer ('unauthorised payment transactions')"
- "Payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee ('manipulation of the payer')." Payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order are often referred to as scams.

Source for definitions of 'unauthorised payment transactions' and 'manipulation of the payer': Guideline 1.1 of the European Banking Authority's Guidelines on reporting requirements for fraud data under Article 96(6) PSD2.



7. Initiator (who)

Initiator (who)		
Describes who initiates the payment transaction affected by the fraud (aligned with EBA Guidelines on Fraud Reporting under PSD2)		
	Definition	**Example**
Customer	Manipulation of the payer by the fraudster to issue a payment order. Source: Guidelines EBA/GL/2018/05 (consolidated version) on Fraud Reporting under PSD2 (Art. 96(6))[1] "b. payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee ('manipulation of the payer')." (Guideline 1.1 b.: Payment transactions and fraudulent payment transactions)	• Manipulation of the customer into initiating and signing off a payment order

[1] https://eba.europa.eu/sites/default/documents/files/document_library//Guidelines amending EBA GL on Fraud reporting under PSD2.pdf https://www.eba.europa.eu/sites/default/documents/files/document_library/960425/Final%20Report%20on%20EBA%20GL%20on%20fraud%20reporting%20-%20Consolidated%20version.pdf

Initiator (who) (continued)		
Describes who initiates the payment transaction affected by the fraud (aligned with EBA Guidelines on Fraud Reporting under PSD2)		
	Definition	**Example**
Fraudster	Issuance of a payment order by the fraudster. Source: Guidelines EBA/GL/2018/05 (consolidated version) on Fraud Reporting under PSD2 (Article. 96(6)) "c. 'Modification of a payment order by the fraudster' is a type of unauthorised transaction as defined in Guideline 1.1(a) and refers to a situation where the fraudster intercepts and modifies a legitimate payment order at some point during the electronic communication between the payer's device and the payment service provider (for instance through malware or attacks allowing attackers to eavesdrop on the communication between two legitimately communicating hosts (man-in-the middle attacks)) or modifies the payment instruction in the payment service provider's system before the payment order is cleared and settled." (Guideline 1.6 c.: Payment transactions and fraudulent payment transactions) "d. 'Issuance of a payment order by the fraudster' is a type of unauthorised transaction as defined in Guideline 1.1(a) and refers to a situation where a fake payment order is issued by the fraudster after having obtained the payer/payee's sensitive payment data through fraudulent means." (Guideline 1.6 d.: Payment transactions and fraudulent payment transactions)	• Initiation and sign-off of a payment order by the fraudster • Manipulation of the customer into signing off a payment order initiated by the fraudster

Initiator (who) (continued)		
Describes who initiates the payment transaction affected by the fraud (aligned with EBA Guidelines on Fraud Reporting under PSD2)		
	Definition	**Example**
First party (optional element relevant, in particular, to card fraud)	"First-party fraud is where a person knowingly misrepresents their identity or gives false information for financial or material gain." Source: Experian 'The different types of fraud and how they're changing' https://www.experian.co.uk/blogs/latest-thinking/fraud-prevention/what-is-first-second-and-third-party-fraud/ This is usually done when applying for a product or service to receive more favourable rates, or if they have no intention of meeting their commitments.	Fraudulent online credit card application

8. Method (how)

Method (how)		
Describes the attack vector and specifies the first point of contact between the fraudster and the victim or the point of compromise.		
Name of method	**High-level description**	**Example**
Brute force	"An unsophisticated and exhaustive process to try and determine a cryptographic key or password without the user's knowledge by systematically trying all alternatives or combinations until the correct one is discovered." Source: Australian Cyber Security Centre 'Glossary' https://www.cyber.gov.au/learn-basics/view-resources/glossary/b	BIN attack
Data breach / theft	"A **data breach** is a security incident in which information is accessed without authorization." Source: Norton 'What is a data breach?' https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html **"Data theft** is the act of stealing information stored on corporate databases, devices, and servers. This form of corporate theft is a significant risk for businesses of all sizes and can originate both inside and outside an organization." Source: Okta 'What is Data Theft?' https://www.okta.com/blog/2020/07/data-theft/	Theft of customer data/credentials from a merchant database
E-mail compromise	Use of hacked or spoofed e-mail address to gain access to other parties for fraudulent purposes: "Business Email Compromise (BEC) is a type of scam targeting companies who conduct wire transfers and have suppliers abroad. Corporate or publicly available email accounts of executives or high-level employees related to finance or involved with wire transfer payments are either spoofed or compromised through keyloggers or phishing attacks to do fraudulent transfers (…)" Source: Trend Micro 'Business Email Compromise (BEC)' https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)	Used for CEO fraud

Method (how) (continued)		
Describes the attack vector and specifies the first point of contact between the fraudster and the victim or the point of compromise.		
Name of method	**High-level description**	**Example**
E-mail contact	The first point of contact was an e-mail message from the fraudster to the victim.	
Fake advertising	The fraudster has created advertisement, which lures victims in with false promises.	Direct advertisement in the form of banners and pop-ups Fraudulent web pages that are created with the objective to incentivise the victim to contact the fraudster
Fake merchant	Fake merchant websites, for example, offering non-existing goods or services to harvest personal details or banking / card details (honey trap) or to make the victim initiate a payment transaction.	
In person contact	The first point of contact was a person-to-person contact between the fraudster and the victim initiated by the fraudster.	
Malware	"'Malware' is short for malicious software and used as a single term to refer to virus, spy ware, worm etc. Malware is designed to cause damage to a stand-alone computer or a networked pc. So wherever a malware term is used it means a program which is designed to damage your computer[;] it may be a virus, worm or Trojan." Source: Digicert 'What are Malware, Viruses, Spyware, and Cookies?' https://www.websecurity.digicert.com/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them	Modification of a payment order by the fraudster

Method (how) (continued)		
Describes the attack vector and specifies the first point of contact between the fraudster and the victim or the point of compromise.		
Name of method	**High-level description**	**Example**
Online contact	Contact while "connected to, served by, or available through a system and especially a computer or telecommunications system (such as the Internet)" Source: Merriam Webster https://www.merriam-webster.com/dictionary/online#other-words. This online contact would usually be initiated by the first-party fraudster with an online helpdesk or service centre at a financial institution.	Online credit card application, fraudulent disputes
Phone contact	The first point of contact was a phone call by the fraudster to the victim.	
Physical copy	Creation of a physical duplicate or taking of a picture of a card or key card.	Skimming
Physical theft	Physical stealing of access credentials or device or whatever is needed to create fraud.	
Social media compromise	Use of hacked, spoofed or stolen social media accounts to gain access to other parties for fraudulent purposes.	
Social media contact	The first point of contact was a message from the fraudster to the victim via a social media channel.	Instagram, Facebook, Snapchat, LinkedIn
Text message contact (includes any form of pure text that is designed for messaging)	The first point of contact was a text message from the fraudster to the victim sent through a (pure) text messaging functionality/app.	SMS, iMessage, WhatsApp
New method	Used to register a new method of contact / attack vector not yet included in the list of methods	

9. Modus (what)

Modus (what)
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"Your money / personal information is at risk":** Fraudster tricks victim into believing that an intervention is needed to keep their money / personal information safe.

Name of modus	Definition	Possible Labels/Tags*
Safe account fraud	"You'll usually [be] contacted by someone saying they are from the bank or the police. They'll (…) ask you to transfer your money to a "safe account" they have set up on your behalf. The account will belong to a fraudster." Source: Barclays Bank UK 'Ten common types of fraud and scam – 9. Safe account fraud' https://www.barclays.co.uk/smart-investor/new-to-investing/reducing-unnecessary-risk/ten-common-types-of-fraud-and-scam/#back=%2Fcontent%2Fbarclaysuk%2Fen%2Fhelp%2Fresults.html%3Fq%3DSafe%2Baccount%2Bfraud%26_charset_%3DUTF-8%26offset%3D0%26origin%3Dhelp.barclays.co.uk Alternatively/additionally, this modus could result in the victim handing over account credentials or card details and/or completing authentication steps required to access the account and/or sign off payment transactions.	• Fake bank / financial institution • Fake police • Impersonation

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) (continued)
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"Your money / personal information is at risk" (continued):** Fraudster tricks victim into believing that an intervention is needed to keep their money / personal information safe..

Name of modus	Definition	Possible Labels/Tags*
Stop unauthorised transaction fraud	"The fraudster impersonates a bank or police representative and tells the bank customer that an unauthorised transaction can be blocked by giving out authentication codes and/or signing off transactions and/or sending money." Source: EGPF	• Fake bank / financial institution • Fake police • Impersonation
Stop unauthorised access fraud	"The fraudster impersonates a representative of a payment service provider, police or a public authority. The fraudster tells the bank customer that someone has gained unauthorised access to the customer's accounts and therefore, the customer would be exposed to multiple risks. The fraudster convinces the bank customer that this unauthorised access can be addressed by the customer authenticating themselves or providing authentication codes." Source: EGPF	• Fake bank / financial institution • Fake police • Impersonation

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) (continued)
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"You can earn/save a lot of money":** Victim makes payment up front in expectation of a return at a later stage.

Name of modus	Definition	Possible Labels/Tags*
Advance fee fraud (does not include twists)	"Advance fee fraud is when fraudsters target victims to make advance or upfront payments for goods, services and/or financial gains that do not materialise." Source: National Fraud & Cyber Crime Reporting Centre 'Advance Fee Fraud' https://www.actionfraud.police.uk/a-z-of-fraud/advance-fee-fraud Alternatively / additionally, this modus could result in the victim handing over account credentials or card details and/or completing authentication steps required to access the account and/or sign off payment transactions.	• Fake betting • Fake loan • Fake prize, sweepstakes and lottery scams • Impersonation • Nigeria
Claim a benefit fraud	"The aim of this type of fraud is to deceive victims into handing over account credentials or card details and/or completing authentication steps required to access the account and/or sign off payment transactions to claim a reward or benefits, such as lottery wins, discounts or reimbursements." Source: EGPF	• Discount / refund fraud • Fake customer support • Fake prize, sweepstakes and lottery scams • Impersonation

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) (continued)
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"You can earn/save a lot of money" (continued):** Victim makes payment up front in expectation of a return at a later stage.

Name of modus	Definition	Possible Labels/Tags*
Investment fraud	"Investment schemes involve promises of big payouts, quick money or guaranteed returns." Source: Australian Competition & Consumer Commission (ACCC) 'Investment scams' https://www.scamwatch.gov.au/types-of-scams/investments/investment-scams	• Fake website • Fraudulent use of Contract for Difference (CFD) • Fraudulent use of crypto currency • Impersonation • Non-crypto investment scam

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) (continued)
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"I am a seller/buyer":** Victim responds to fake/alleged offer for services/goods that later turns out to be fraudulent.

Name of modus	Definition	Possible Labels/Tags*
Online shopping fraud	"Shopping and auction fraud involves fraudulent shopping scams that rely on the anonymity of the internet." Source: National Fraud & Cyber Crime Reporting Centre 'Online shopping fraud' https://www.actionfraud.police.uk/a-z-of-fraud/online-shopping-fraud Examples: • buyers not receiving goods • sellers not receiving payment • buyers receiving goods that are either less valuable than those advertised or significantly different from the original description • failure to disclose relevant information about a product or the terms of sale	• Fake website • Goods not received • Lookalike domain

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) (continued)
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"Please help me":** Fraudster creates an emotional bond with the victim, typically friendship/sympathy/romantic, then exploits the bond by getting the victim to help the fraudster financially.

Name of modus	Definition	Possible Labels/Tags*
Emotional manipulation	"Scammers (...) play on emotional triggers to get you to provide money, gifts or personal details." Source: Australian Competition & Consumer Commission (ACCC) 'Dating and romance' https://www.scamwatch.gov.au/types-of-scams/dating-romance. Alternatively/additionally, this modus could result in the victim handing over account credentials or card details and/or completing authentication steps required to access the account and/or sign off payment transactions.	• Impersonation • Romance scam

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) (continued)
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"Send me money or I'll …":** Fraudster extorts e.g. money from victim, based on exposure threat, blackmail or other, like ransomware.

Name of modus	**Definition**	**Possible Labels/Tags***
Extortion	"Threats to life, arrest or other involve demands by scammers to pay money that you supposedly owe and threats if you do not cooperate." Source: Australian Competition & Consumer Commission (ACCC) 'Threats to life, arrest or other' https://www.scamwatch.gov.au/types-of-scams/threats-extortion/threats-to-life-arrest-or-other. Alternatively/additionally, this modus could result in the victim handing over account credentials or card details and/or completing authentication steps required to access the account and/or sign off payment transactions.	• Nightclub • Ransomware • Sextortion

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) (continued)
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"We've changed account number":** Victim misled into replacing genuine static account details of a creditor with details of an account under control of a fraudster.

Name of modus	Definition	Possible Labels/Tags*
Impersonation of creditor	"A fraudster impersonates a service provider, supplier or other creditor and tricks the victim into making a bill payment to an account that is not the account of the actual creditor but the account of the fraudster." Source: EGPF	• Beneficiary account change • Impersonation

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) (continued)
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"You owe money":** Fraudster makes victim believe money is owed or due, usually in relation to completely fictitious transactions or payments.

Name of modus	Definition	Possible Labels/Tags*
Overpayment scams	"Overpayment scams work by getting you to 'refund' a scammer who has sent you too much money for an item you are selling." Source: Australian Competition & Consumer Commission (ACCC) 'Overpayment scams' https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/overpayment-scams	• Card not present (scammer paid with lost or stolen card)
Phoney debt/bill collection	"Aggressive fake debt collectors, who try to bully their targets into paying money they don't owe." Source: AARP 'Debt Collection Scams' https://www.aarp.org/money/scams-fraud/info-2019/debt-collector.html	• CEO fraud • False billing scam • Manipulated invoice • Subscription scam

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) continued
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **"Can you please sign this?":** Fraudster tricks customer into giving out authentication codes for seemingly legitimate reasons not related to bank activity.

Name of modus	**Definition**	**Possible Labels/Tags***
Fake institution	"The fraudster impersonates or claims to act on behalf of an institution like a health care provider or a government agency. The fraudster asks the customer to provide authentication data and/or go through authentication steps in order to e.g., identify themselves, sign something, or confirm something. The customers believe that they are resolving a legitimate issue by engaging with the fraudster." Source: EGPF.	• Impersonation • Fake bank / financial institution • Fake police

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) continued
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **Account takeover:** Account takeover by unauthorised party.

Name of modus	Definition	Possible Labels/Tags*
Pure account takeover	"An account takeover can happen when a fraudster or computer criminal poses as a genuine customer, gains control of an account and makes unauthorised transactions. (…) Online banking accounts are usually taken over as a result of phishing, spyware or malware scams (…)" Source: National Fraud & Cyber Crime Reporting Centre 'Account takeover' https://www.actionfraud.police.uk/a-z-of-fraud/account-takeover Pure account takeover is a form of account takeover where the fraudster gains access to the account without tricking the victim into a handover of credentials. Example: stealing of authentication device.	• Account takeover • Physical proximity credential theft
Creditor account data manipulation	"Creditor account data manipulation occurs if, following an account takeover, the fraudster changes creditor account data stored in this account so that future transactions reach the wrong beneficiaries." Source: EGPF.	• Account takeover • Beneficiary account change

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) continued
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **Card fraud**

Name of modus	Definition	Possible Labels/Tags*
Card details stolen	"...involves the unauthorised use of credit or debit data (the card number, billing address, security code and expiry date) to purchase products and services in a non-face-to-face setting, such as via e-commerce websites or over the telephone." Source: Europol 'Payment Fraud' https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud	• Account takeover • Advanced persistent threat (APT) • BIN attack • Card not present • Card peeking • Card skimming • Collusive merchant data misuse • Contactless relay fraud • Credit master • Fraudulent MOTO card transaction • Keylogger • Malware – MageCart • Physical proximity credential theft • Shoulder surfing • Third-party vendor account takeover

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) continued
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **Card fraud (continued)**

Name of modus	**Definition**	**Possible Labels/Tags***
Card lost or stolen	"Fraud carried out on cards that have been lost or stolen. There are various ways that criminals try to steal cards [or PINs]: intercepting new cards or card PINs in the post, handbag or wallet snatches, shoulder surfing, distraction theft." Source: FraudSmart 'Lost or Stolen Cards https://www.fraudsmart.ie/personal/fraud-scams/card-cheque-fraud/lost-or-stolen-cards/	• Account takeover • Wecycle
Card never received	"when a new or replacement card is stolen from the mail, never reaching its rightful owner." Source: Digital News Asia 'The 8 Different Types of Card Fraud'https://www.digitalnewsasia.com/insights/the-8-different-types-of-card-fraud?8d5f_name=ff	• Account takeover

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) continued
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **Card fraud (continued)**

Name of modus	Definition	Possible Labels/Tags*
Use of counterfeit cards	"Counterfeit cards are fake credit cards with an actual account's info that can be gained through various methods. A lot of times the victims of these crimes will still have their actual cards and never realize that their information was stolen. These cards might appear to be genuine and even have the issuers' logos along with the encoded magnetic strips." Source: Fraud.net 'Fraud Definitions / Counterfeit Card' https://fraud.net/d/	• Account takeover • Advanced persistent threat (APT) • Card peeking • Card present • Card skimming • Fraudulent MOTO card transaction • Physical proximity credential theft • Shoulder surfing
Fraudulent card application	"when a fraudster uses another person's name and information to apply for and obtain a credit card." Source: Digital News Asia 'The 8 Different Types of Card Fraud' https://www.digitalnewsasia.com/insights/the-8-different-types-of-card-fraud?8d5f_name=ff	• Falsified ID • Falsifying personal and financial information • First party • Impersonation • Synthetic ID

*****Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) continued
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **Card fraud (continued)**

Name of the modus	**Definition**	**Possible Labels/Tags***
Fraudulent card claim	The fraudster files a false credit card dispute claim e.g. false chargebacks. “Cardholders are entitled to chargebacks in cases of criminal fraud or merchant abuse. (…) chargeback abuse occurs if a buyer files a chargeback claim that’s not tied to one of those valid reasons. (…) Chargeback abuse is also known as first-party fraud, or “friendly” fraud. This describes any situation in which a cardholder files a false chargeback claim without justification.” Source: Charbebacks911.com ‘False Chargeback Claims’ https://chargebacks911.com/false-chargeback-claims/ Examples: • Impersonating the victim or pretending to be a victim, the fraudster presents a fraudulent claim to the bank.	• Exploiting the system • First party

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

Modus (what) continued
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction
High-level classification: **Card fraud (continued)**

Name of modus	Definition	Possible Labels/Tags*
Fraudulent use of cash back scheme	Fraudulent use of cash back schemes involves fake transactions between merchants and employees to make undue gains from cashback offers. "Cash back is commonly used by credit cards. Whenever customers use their credit cards to make a purchase, they get back cash, based on certain conditions." Source: Global Banking & Finance Review 'What is cash back?' https://www.globalbankingandfinance.com/what-is-cash-back/	• Exploiting the system • First party

Modus (what) continued	
Describes the unauthorised and often manipulative action taken by the fraudster and resulting in the loss of money via a payment transaction	
High-level classification: **"Tag line for new fraud type"**	
New fraud type (describe)	Used to register new modus not yet included in the list of modi

***** Individual PSPs remain free to choose labels/tags as they deem fit, for example to align with internal reporting requirements. The possible labels/tags set out here are suggestions only.

10. Labels/tags (PSP individual)

The labels/tags listed below are suggestions and not meant to be exhaustive.

Label/tag (PSP individual)		
Can be freely chosen by individual PSPs and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Account takeover	"Account takeover fraud is a form of identity theft in which the fraudster gets access to a victim's bank or credit card accounts — through a data breach, malware or phishing — and uses them to make unauthorized transactions." Source: Credit Cards.com 'Credit Card Glossary: Terms and Definitions – Account takeover fraud' https://www.creditcards.com/credit-card-news/glossary/term-account-takeover-fraud/	
Advanced persistent threat (APT)	"An advanced persistent threat (APT) is a covert cyber attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period. During the time between infection and remediation the hacker will often monitor, intercept, and relay information and sensitive data." Cisco 'What Is an Advanced Persistent Threat (APT)?' https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html	
Beneficiary account change	"A beneficiary change request is a request to change the details of a beneficiary's account or accounts to which payments are made. A fraudster exploits weaknesses in a genuine change request process, changing genuine beneficiary account details to those of an account or accounts that he holds." Source: Citibank 'Beneficiary Change Request: Risks and Best Practices' https://www.citibank.com/tts/sa/emea_marketing/docs/Beneficiary-Change-Request-Risks-and-Best-Practices.pdf	

Label/tag (PSP individual)		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
BIN attack	"Credit cards are produced in BIN ranges. Where an issuer does not use random generation of the card number, it is possible for an attacker to obtain one good card number and generate valid card numbers." Source: European Association for Secure Transactions (EAST) 'Fraud Definitions' https://www.association-secure-transactions.eu/industry-information/fraud-definitions/	
Card not present	Fraudulent action takes place as part of a card not present transaction: "A card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC) is a payment card transaction made where the cardholder does not or cannot physically present the card for a merchant's visual examination at the time that an order is given and payment effected." Source: European Association for Secure Transactions (EAST) 'Fraud Definitions' https://www.association-secure-transactions.eu/industry-information/fraud-definitions/	
Card peeking	"Card details stolen by someone who has physical access to the card. The card remains in the possession of the cardholder." Source: EGPF.	An employee has their business card stored in their office drawer. A colleague is able to get necessary card information without stealing the physical card.
Card present	Fraudulent action takes place as part of a card present transaction: "A card present transaction occurs when a cardholder physically presents a card to request and authorise a financial transaction.". Source: European Association for Secure Transactions (EAST) 'Fraud Definitions' https://www.association-secure-transactions.eu/industry-information/fraud-definitions/	

Label/tag (PSP individual)		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Card skimming	"Skimming occurs when devices illegally installed on ATMs, point-of-sale (POS) terminals, or fuel pumps capture data or record cardholders' PINs. Criminals use the data to create fake debit or credit cards and then steal from victims' accounts." Source: FBI 'Scams and Safety' https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/skimming	
CEO fraud	"CEO fraud will typically start with an email being sent from a fraudster to a member of staff in a company's finance department. The member of staff will be told by the fraudster who is purporting to be a company director or CEO that they need to quickly transfer money to a certain bank account for a specific reason. The member of staff will do as their boss has instructed, only to find that they have sent money to a fraudster's bank account. The fraudster will normally redistribute this money into other mule accounts and then close down the bank account to make it untraceable." Source: National Fraud & Cyber Crime Reporting Centre 'Action Fraud warning after serious rise in CEO fraud' https://www.actionfraud.police.uk/alert/action-fraud-warning-after-serious-rise-in-ceo-fraud	Impersonation of manager
Collusive merchant / data misuse	"This type of fraud occurs when merchant owners and/or their employees conspire to commit fraud using their customers' (cardholder) accounts and/or personal information. Merchant owners and/or their employees pass on the information about cardholders to fraudsters." Source: Cards Business Review#2003–01, 'Understanding Credit Card Frauds', Tej Paul Bhatla, Vikram Prabhu & Amit Dua[2]	*Note: this fraudulent behaviour could also occur by abusing existing direct debit mandates or issuing new direct debit mandates*

[2] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.431.7770&rep=rep1&type=pdf

Label/tag (PSP individual)		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Contactless relay fraud	"Where a fraudster uses a mobile NFC POS terminal or smartphone to capture a payment by standing very close to the cardholder in a public place and reading their contactless card through their clothing or handbag." Source: EGPF	
Credit master	"Algorithms are deployed which automatically generate credit card account numbers from an existing correct number as well as pairs of expiration dates. The criminal software then automatically tests these combinations, working sequentially through number combinations to see which match genuine cards by attempting a transaction." Global Banking & Finance Review 'Fraud: the artificial intelligence arms race is on' https://www.globalbankingandfinance.com/fraud-the-artificial-intelligence-arms-race-is-on/	
Discount / refund fraud	"The fraudster impersonates customer support and convinces the victim that they are entitled to a discount, they just have to authenticate themselves first, thus giving the fraudster access to their account and/or signing off unauthorised transactions." Source: EGPF	
Exploiting the system	"The cardholder is trying to benefit and avoid paying for goods/services by filing a dispute and using the chargeback system." Source: EGPF	

Label/tag (PSP individual)		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Fake bank / financial institution	Victim receives e.g. “phone calls or messages with the caller or sender claiming to be from (…) banks (…), prompting the recipient to act on a matter that requires immediate attention. By creating a sense of urgency, these impersonation scams take advantage of victims’ fears.” Source: Channel News Asia ‘Impersonation scams: How familiarity can be used against you’ https://www.channelnewsasia.com/news/advertorial/impersonation-scams-how-familiarity-can-be-used-against-you-13340804	Someone calls and pretends to represent a financial institution. “A common ploy involves the scammer impersonating a bank representative and calling to check on fraudulent charges detected in a bank account. The impersonator would gain the victim’s trust by offering their help to resolve these issues. Caught unaware and fearful that their bank account might be compromised, these victims would follow the instructions of the scammer and provide their personal details, only to realise afterwards that they have been conned.” (Channel News Asia, Impersonation scams: How familiarity can be used against you)

Label/tag (PSP individual)		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Fake betting	"Betting and sports investment scams try to convince you to invest in foolproof systems and software that can 'guarantee' a profit on sporting events. (…) Betting syndicates: The scammer will try and convince you to become a member of a betting syndicate. You will need to pay a compulsory fee (…) to join and open a sports betting account. You will be required to make ongoing deposits to maintain the balance of the account. The scammer tells you that they will use funds in the account to place bets on behalf of the syndicate. You, and other 'syndicate members' are promised a percentage of the profits." Source: Australian Competition & Consumer Commission (ACCC) 'Betting & sports investment scams' https://www.scamwatch.gov.au/types-of-scams/investments/betting-sports-investment-scams	Fake betting scams often involve social media chats where it is promised that a winner is known. The victim is invited to become a member of a group which promises successful bets subject to paying a fee.
Fake customer support	Fraudster impersonates customer support "The scammer will phone you and pretend to be a staff member from a large telecommunications or computer company (…). Alternatively they may claim to be from a technical support service provider. They will tell you that your computer has been sending error messages or that it has a virus. (…) The caller will request remote access to your computer to 'find out what the problem is'. The scammer may try to talk you into buying unnecessary software or a service to 'fix' the computer, or they may ask you for your personal details and your bank or credit card details." Source: Australian Competition & Consumer Commission (ACCC) 'Remote access scams' https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/remote-access-scams	

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Fake loan	"In an advance-fee loan scam, scammers promise they'll get you a loan, credit card, or access to credit. Or they say they'll put you in touch with a lender who can almost certainly get you those things. No matter your credit history. But first, they say, you must pay up front. The scammer may say the money is a fee for "processing," "insurance," an "application," or something else. But it's a lie. There is no loan and there is no lender. And if you pay, the scammer and your money will disappear. Source: US Federal Trade Commission 'What To Know About Advance-Fee Loans' https://www.consumer.ftc.gov/articles/what-know-about-advance-fee-loans	
Fake police	"To identify yourself as an officer of the law to purposefully deceive other individuals and gain advantage through such deceit. Impersonation may include dressing as an officer of the law or simply falsely identifying oneself as an officer to someone else." Source: Hart Powell 'Impersonating a Police Officer' https://www.kohlerandhart.com/articles/impersonating-a-police-officer/	Scammers impersonate a police officer
Fake prize, sweepstakes, and lottery scams	"Lottery, sweepstake or prize draw fraud happens after fraudsters contact you to tell you you've won a large sum of money in an international lottery, sweepstake or other prize draw. (…) However, either the lottery doesn't exist or you've been contacted by fraudsters misusing the name of a genuine lottery. (…) If you respond to the fraudster, you'll be asked to supply personal information and copies of official documents, such as your passport, as proof of identity. The fraudsters can then use this information to steal your identity. Once you have provided your personal information, the fraudsters will ask you to pay various fees – for example: taxes, legal fees, banking fees etc. – so that they can release your non-existent winnings. (…) The fraudsters may also ask for your bank details, saying they will pay your winnings directly into your bank account. But if you hand over your bank details, the fraudsters will use them to empty your account." Source: National Fraud & Cyber Crime Reporting Centre 'Lottery scams' https://www.actionfraud.police.uk/a-z-of-fraud/lottery-scams	

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Fake website	"Fake sites made to look like real ones to steal your personal or banking details when you submit them to the site." Source: Metropolitan Police 'Online shopping' https://www.met.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/online-shopping/?__cf_chl_captcha_tk__=3t_OKD9aWynQUGBzQ5_yr13Pld3pZH609uXmTvTZyUQ-1641809644-0-gaNycGzNCH0	
False billing scam	"False billing scams request you or your business to pay fake invoices for directory listings, advertising, domain name renewals or office supplies that you did not order." Source: Australian Competition & Consumer Commission (ACCC) 'False billing' https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/false-billing	
Falsified ID	"A false or fake ID is any form of identification that is forged, altered, or otherwise purports to establish the false identity of a person." Source: Criminal Defense Lawyer 'Fake ID: Laws and Penalties'[3]	
Falsifying personal and financial information	"Falsification is the act of deliberately lying about or misrepresenting something." Source: Vocabulary.com https://www.vocabulary.com/dictionary/falsification	
First party	"First party fraud is where a person knowingly misrepresents their identity or gives false information for financial or material gain." Source: Experian 'The different types of fraud and how they're changing' https://www.experian.co.uk/blogs/latest-thinking/fraud-prevention/what-is-first-second-and-third-party-fraud/ This is usually done when applying for a product or service to receive more favourable rates, or if they have no intention of meeting their commitments.	

[3] https://www.criminaldefenselawyer.com/resources/criminal-defense/juvenile/fake-id-laws-and-penalties.htm#:~:text=A%20false%20or%20fake%20ID,driver's%20license%20on%20your%20computer .

Label tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Fraudulent MOTO card transaction	"... fraud in so-called "card-not-present" transactions online or via email order and telephone transactions." Source: Digital News Asia 'The 8 Different Types of Card Fraud' https://www.digitalnewsasia.com/insights/the-8-different-types-of-card-fraud?8d5f_name=ff	
Fraudulent use of Contract for Difference (CFD)	"Contracts for difference (CFD) are a popular way of trading on the price of stocks and indices, commodities, forex and cryptocurrencies without owning the underlying assets. (…) A CFD is a contract between a broker and a trader who agree to exchange the difference in value of an underlying security between the beginning and the end of the contract, often less than one day." Source: Capital.com 'What is CFD trading and how does it work?' https://capital.com/what-is-cfd-trading	Fraudster pretends to represent a legitimate company offering an investment opportunity based on CFD. The customer is directed to a fake website where he/she is tricked into setting up an account. Once the customer wishes to liquidate the account, the funds are gone.
Fraudulent use of crypto currency	"Cryptocurrency is a type of digital currency that generally exists only electronically. You usually use your phone, computer, or a cryptocurrency ATM to buy cryptocurrency. Bitcoin and Ether are well-known cryptocurrencies, but there are many different cryptocurrencies, and new ones keep being created. … with investment scams, crypto is central in two ways: it can be both the investment and the payment" Source: U.S. Federal Trade Commission 'What To Know About Cryptocurrency and Scams' https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams	Fraudster pretends to represent a legitimate company offering an opportunity to invest into crypto currency. The customer is directed to a fake website where he/she is tricked into setting up an account. Once the customer wishes to liquidate the account, the funds are gone.

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Gift card	"Scammers like to get gift cards as payment as it's easy for them to quickly sell them on secondary markets and pocket the cash." Source: Australian Competition & Consumer Commission (ACCC) 'Payment demanded by gift card? It's a scam' https://www.scamwatch.gov.au/news-alerts/payment-demanded-by-gift-card-its-a-scam	
Goods not received	Payer submitted payment, however, does not receive the purchased goods, because offer was issued on a fake website store or by a fake seller. "Fake websites/stores: scammers will set up fake online stores, on websites or social media, which can look like genuine online retailers. Many of these offer luxury items at very low prices but you may receive a fake item or nothing at all. Fake sellers: scammers may pose as genuine sellers on classifieds websites. The scammer may claim they are travelling and an agent will deliver the goods once you have paid, but you won't receive the goods and will be unable to contact the seller." Source: Australian Competition & Consumer Commission (ACCC) "Tis the season for online shopping scams' https://www.scamwatch.gov.au/news-alerts/tis-the-season-for-online-shopping-scams	
Impersonation	"the act of attempting to deceive someone by pretending that you are another person" Source: Cambridge Dictionary https://dictionary.cambridge.org/dictionary/english/impersonation	
Keylogger	"A keylogger (or keystroke logger) is a type of software or hardware used to track and record what someone types on theirkeyboard." Source: Norton 'Keyloggers 101: A definition + keystroke logging detection methods' https://us.norton.com/internetsecurity-malware-what-is-a-keylogger.html	

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Lookalike domain	"Lookalike or 'cousin' domain names are addresses that use character replacement to make them look as close as possible to the domain of a brand, service or government authority. For example, characters in a domain name such as an "l" can be replaced with a "1", or the letter l with the number 1. These names are most often registered by third parties up to mischief. You can imagine why this practice is problematic and the issues it can cause. While close inspection of a domain name will often reveal the issue, a cursory glance might overlook it. (…) Some also include misspellings in the definition of lookalike domains." Source: Domain Registration Services Domain Name Registrar (Australia) 'What is a lookalike domain name?'[4]	Fraudsters create domains that are very similar to those of existing businesses or financial institutions but include small differences in e.g. spelling of the business' name. With the help of these domain names, fraudsters collect, among others, sign-in credentials from customers for online payment or shopping accounts.
Malware – MageCart	"Magecart is a consortium of malicious hacker groups who target online shopping cart systems, usually the Magento system, to steal customer payment card information. This is known as a supply chain attack. The idea behind these attacks is to compromise a third-party piece of software from a VAR or systems integrator or infect an industrial process unbeknownst to IT." Source: CSO 'What is Magecart? How this hacker group steals payment card data' https://www.csoonline.com/article/3400381/what-is-magecart-how-this-hacker-group-steals-payment-card-data.html	

[4] https://www.domainregistration.com.au/news/2020/0409-lookalike-domains.php#:~:text=Domain%20Name%20News&text=Lookalike%20or%20%22cousin%22%20domain%20names,l%20with%20the%20number%201.

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Manipulated invoice	"A contractor or supplier can commit fraud by knowingly submitting false, inflated or duplicate invoices with the intent to defraud, either acting alone or in collusion with contracting personnel as the result of corruption. 'False invoices' refer to invoices for goods or services not rendered. 'Duplicate invoices' are fraudulent if issued knowingly with the intent to defraud." Source: Guide to Combating Corruption & Fraud in Development Projects 'Potential Scheme: False, Inflated and Duplicate Invoices', https://guide.iacrc.org/potential-scheme-false-inflated-and-duplicate-invoices/ .	
Multiple imprint	"when a single transaction is recorded multiple times on old-fashioned credit card imprint machines known as "knuckle busters". Source: Digital News Asia 'The 8 Different Types of Card Fraud' https://www.digitalnewsasia.com/insights/the-8-different-types-of-card-fraud?8d5f_name=ff	
Nigeria	Nigerian or unexpected money scams "involve someone overseas offering you a share in a large sum of money or a payment on the condition you help them to transfer money out of their country." Source: Australian Competition & Consumer Commission (ACCC) 'Unexpected money scams' https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams	
Nightclub	"Clip joint scam or nightclub scam where customers are threatened by a nightclub they have visited into making payments." Source: EGPF	

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Non-crypto investment scam	"You're looking to buy a bond or shares, or researching what to do with your pension money (…). You're then contacted by someone offering a good deal – often tailored for you – and they have documents that look genuine. You might be asked to pay an up-front fee to secure the investment. Scammers can create documents, websites and online platforms that look real. They'll do this to make you believe you're dealing with a genuine company. You think you're dealing with a genuine and well-known company, but it's really a scammer posing as them." Source: Barclays Bank UK 'Investment Scams' https://www.barclays.co.uk/fraud-and-scams/investment-scams/	
No physical meeting	"E.g. reunion exclusively using a digital communication channel." Source: EGPF.	
Phishing	"Technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business – a bank, or credit card company – requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate." European Association for Secure Transactions (EAST) 'Fraud Definitions' https://www.association-secure-transactions.eu/industry-information/fraud-definitions/	
Physical meeting	"Face-to-face reunion." Source: EGPF.	

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Physical proximity credential theft / known perpetrator	"Credential theft where the perpetrator is known to the victim." Source: EGPF.	This could be a family member, family friend or caretaker who has been in the vicinity of the victim and e.g. takes a photo of the victim's payment card
Physical proximity credential theft / unknown perpetrator	"Credential theft where the perpetrator is not known to the victim." Source: EGPF.	A person not known to the victim steals the victim's payment card e.g. from the locker in the gym.
Ransomware	"Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers, and can thus quickly paralyze an entire organization." Source: Trellix 'What Is Ransomware?' https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html	

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Remote access trojan	"A malicious program that remotely accesses infected resources. Trojans of this type are among the most dangerous because they open up all kinds of opportunities for remote control of the compromised system. RAT capabilities usually include program installation and removal, file manipulation, reading data from the keyboard, webcam hijacking, and clipboard monitoring." Source: Kaspersky IT Encyclopedia 'Remote access trojan' https://encyclopedia.kaspersky.com/glossary/remote-access-trojan-rat/	
Romance scam	"Scammers take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be prospective companions. They play on emotional triggers to get you to provide money, gifts or personal details." Source: Australian Competition & Consumer Commission (ACCC) 'Dating and Romance' https://www.scamwatch.gov.au/types-of-scams/dating-romance	
Sextortion	"Scammers are using social media platforms and email as forums for sextortion scams, where they threaten to share intimate images or footage of you online, unless you give in to their demands." Source: Australian Competition & Consumer Commission (ACCC) 'Gen Z the fastest growing victims of scams' https://www.scamwatch.gov.au/news-alerts/gen-z-the-fastest-growing-victims-of-scams	
Shoulder surfing	"Shoulder surfing is a criminal practice where thieves steal your personal data by spying over your shoulder as you use a laptop, ATM, public kiosk or other electronic device in public." Source: Experian 'What Is Shoulder Surfing?' https://www.experian.com/blogs/ask-experian/what-is-shoulder-surfing/	

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Smishing	"Also known as "SMS Phishing", is a form of criminal activity using social engineering techniques. SMS phishing uses cell phone text messages to deliver information and/or requests to induce people to divulge or to take action that will compromise their personal or confidential information." Source: European Association for Secure Transactions (EAST) 'Fraud Definitions' https://www.association-secure-transactions.eu/industry-information/fraud-definitions	
Subscription scam	"Some online subscription companies employ confusing business tactics, such as opting customers into recurring charges without their knowledge." Source: CNBC 'Buyer beware: Online lingerie retailer Adore Me under fire by FTC over 'deceptive' subscription service' https://www.cnbc.com/2018/11/16/locked-in-cnbc-investigates-online-subscription-models.html	
Synthetic ID	"Synthetic identity theft, or synthetic identity fraud, occurs when a criminal creates an identity instead of stealing an existing one. The scam involves mixing real Social Security numbers, or fake numbers, with other pieces of information—names, addresses, and birthdates—to put together an entirely new identity, often using partially fake identity information." Source: LifeLock by Norton 'What Is Synthetic Identity Theft?'[5]	

[5] https://www.lifelock.com/learn-identity-theft-resources-synthetic-identity-theft.html#:~:text=Synthetic%20identity%20theft%2C%20or%20synthetic,of%20stealing%20an%20existing%20one.&text=In%20contrast%2C%20the%20more%20familiar,data%20of%20a%20single%20victim.

Label/tag (PSP individual) continued		
Can be freely chosen by individual banks and allows the detecting party to enrich the case with additional categorisation information.		
	Definition	**Example**
Third-party channel	"The fraudster used a third-party channel under PSD2 to initiate the payment." Source: EGPF.	
Third-party vendor account takeover	"The fraudster is able to log into an online account held by the customer with a third party, i.e. a vendor, where payment information (e.g. card details) is stored. This enables the fraudster to consume digital goods/services or order merchandise and redirect its delivery to their own address." Source: EGPF.	
Vishing	"Also known as "voice phishing", is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward. It is also employed by attackers for reconnaissance purposes to gather more detailed intelligence on a target organisation." European Association for Secure Transactions (EAST) 'Fraud Definitions' https://www.association-secure-transactions.eu/industry-information/fraud-definitions/	
Wecycle	"a new trend in debit card fraud – emails sent to consumers asking them to send in expired debit cards. (…) The email also contains a link to an online form where consumers have to enter their personal information before receiving instructions on where to send the debit card for recycling. With personal information and the debit card, fraudsters can easily get their hands on the victim's money." Source: NL Times 'Warning issued over new debit card fraud' https://nltimes.nl/2015/09/18/warning-issued-new-debit-card-fraud	

11. Review and updating process

1. Annual change cycle

To ensure that the EBA Fraud Taxonomy evolves in line with latest insights provided by fraud experts on how to effectively categorise fraud types, it is subject to a review and updating process. Changes to the EBA Fraud Taxonomy are agreed once annually based on the following process:

- **Consultation process – October:** the EBA invites change requests from EGPF members, fraud experts of EBA member organisations and organisations that have usage rights on the fraud taxonomy. Any party wishing to introduce a change request must use a standard form made available by the EBA. Each change request must specify the reason for the suggested change.
- **Submission of change requests:**
  - **Second week of January:** deadline to submit change requests pertaining to the 'initiator', 'method' and 'modus' sections of the EBA Fraud Taxonomy. The specific deadline to submit a change request will be agreed by the EGPF each year.
  - **Early April:** deadline to submit change requests pertaining to the 'labels/tags' section. A related change request must specify the proposed naming and definition of the new label.
- **Review process – mid-January to mid-April:** the EGPF reviews the change requests received. Organisations that have submitted change requests, but are currently not members of the EGPF, will be invited to join the relevant EGPF meeting to engage in the review process. Following review, the EGPF will recommend an updated version of the EBA Fraud Taxonomy.
- **Adoption of updated version of EBA Fraud Taxonomy – May:** the EBA Board adopts an updated version of EBA Fraud Taxonomy.
- **Communication of updated version of EBA fraud taxonomy – June:** the EBA communicates an updated version of the EBA Fraud Taxonomy to EGPF members, fraud experts of EBA member organisations and organisations that have usage rights on the fraud taxonomy.
- **Implementation of updated version of EBA Fraud Taxonomy by users – deployment by end of December for implementation effective on 1 January of the next calendar year:** users are provided with a six-month lead-time to implement an updated version of the EBA Fraud Taxonomy.

2. Emergency change process

If exceptional circumstances require immediate amendments to the EBA Fraud Taxonomy, the emergency change process applies. In this case, the steps leading to the adoption of an updated version of the EBA Fraud Taxonomy may be expedited as required. The emergency change process is triggered if and when considered necessary or appropriate; by way of illustration, circumstances that could trigger an emergency change process could for example include, but are not limited to, regulatory requirements that point to the need to align the taxonomy in an expedited manner, or payment fraud-related developments with a high degree of proliferation and a potential large-scale impact.

12. Annex: changes since EBA Fraud Taxonomy version 3.1 introduced into version 4.0

Amendments introduced into the 'initiator' and 'method' sections:

Initiator section: 2 definitions updated	**Method section:** 1 definition updated, 1 high-level description updated, 1 method deleted
Updated definitions of 'Fraudster' and 'Customer': • Added 'Modification of a payment order by the fraudster' to the definition of 'Fraudster' • Moved the following example from the definition of 'Customer' to the definition of 'Fraudster' as initiator of the payment transaction: "Manipulation of the customer into signing off a payment order initiated by the fraudster"	Updated definition of 'method' (text in Italics added): "Describes the attack vector and specifies the first point of contact between the fraudster and the victim *or the point of compromise.*" (**clarification**)
	Updated example in high-level description of existing method 'Fake advertising' (**clarification**)
	Deleted existing method 'Man in the middle' (**no longer relevant:** the method 'Malware' normally applies in the context of 'modification of a payment order by the fraudster')

Amendments introduced into the 'modus' section:

Modus section: 2 high-level classifications updated, 2 modi added, definitions of 8 modi updated, possible labels/tags for all modi added
High-level classification 'We've changed account number': definition updated (**clarification**)
Updates to high-level classification 'Your money is at risk' • Updated name to 'Your money / personal information' is at risk' (**align with new fraud trend)** • Updated definition (**clarification**)
New modus: 'Stop unauthorised access fraud' in high-level classification 'Your money / personal information is at risk' (**add-on**)
New modus: 'Claim a benefit fraud' in high-level classification 'You can earn/save a lot of money' **(add-on)**
Definitions of four existing modi updated that refer – in addition to the handover of money – also to the handover of credentials (**clarification**) • Safe account fraud • Advance fee fraud • Extortion • Emotional manipulation
Modus 'Advance fee fraud' in high-level classification 'You can earn/save a lot of money': additional update to definition (new authoritative and publicly available source cited) (**clarification**)
Modus 'Card lost or stolen' in high-level classification 'Card fraud': updated definition (**clarification**)
Modus 'Fake institution' in high-level classification 'Can you please sign this?': updated definition (**clarification**)
Modus 'Impersonation of creditor' in high-level classification 'We've changed account number': updated definition (**clarification**)
'Possible labels/tags' completed for each modus

Amendments introduced into the 'labels/tags' section:

Labels/tags section: 3 labels/tags added, 3 definitions updated
Fake prize, sweepstakes, and lottery scams (**add-on**)
Non-crypto investment scam (**add-on**)
Discount / refund fraud (**add-on**)
Card not present: updated definition (**clarification**)
Card present: updated definition (**clarification**)
Fraudulent use of crypto currency: updated definition (**clarification**)

Amendment introduced into chapter 'Review and updating process': updated timeline regarding launch of the annual change cycle