European Payments Council

2023 Payment Threats and Fraud Trends Report

EPC181-23/Version 1.0 / Date issued: 7 November 2023

Public

Report

2023 Payment Threats and Fraud Trends

EPC181-23
Version 1.0
Date issued: 7/11/2023

European Payments Council

European Payments Council AISBL,
Cours Saint-Michel 30 B-1040 Brussels
T +32 2 733 35 33
Enterprise N°0873.268.927
secretariat@epc-cep.eu

Abstract

This new edition of the threats trends report reflects the recent developments concerning security threats and fraud in the payments landscape over the past year.

Table of Contents

List of tables

List of Figures

Executive Summary

The overall purpose of the EPC is to support and promote European payments integration and development, notably the Single Euro Payments Area (SEPA). The EPC is committed to contribute to safe, reliable, efficient, convenient, economically balanced, and sustainable payments, which meet the needs of payment service users and support the goals of competitiveness and innovation in an integrated European economy. It pursues this purpose through the development and management of pan-European payment and payment-related schemes and the formulation of positions and proposals on European payment issues in constant dialogue with other stakeholders and regulators at the European level and taking a strategic and holistic perspective. Since security is one of the cornerstones of customers' trust in payment systems, the EPC decided to devote a yearly report to the latest trends in security threats impacting payments while also giving an insight on how these (could) lead to payment fraud and how to mitigate related risks. By developing this report, the EPC aims to enhance the security awareness amongst the various stakeholders in the payment ecosystem.

The document provides an overview of the attack landscape outlining the most important threats and other "fraud enablers", including social engineering and phishing, malware, Advanced Persistent Threats (APTs), Distributed Denial of Service (DDoS), botnets, third-parties related and monetisation channels. For each threat or "fraud enabler", an analysis is made on the impact and context and suggested controls and mitigations are described. An overview matrix listing the threats with the main controls and mitigation measures is provided in Annex I.

The description of the threats is followed by a section that elaborates on how the identified threats impact the payment-relevant processes. The types of fraud related to specific payment instruments (cards, SEPA schemes - SEPA Credit Transfer, SEPA Direct Debit, SEPA Instant Credit Transfer - and mobile wallets) and supporting schemes such as SEPA Request-to-Pay, are described in the next section while conclusions are presented in the final section.

The following main conclusions concerning *payment threats and fraud enablers* may be drawn from this report:

- Social engineering attacks and phishing attempts are still increasing, and they remain instrumental often in combination with malware, with a shift from consumers, retailers, SMEs to company executives, employees (through "CEO fraud"), payment service providers (PSPs) and payment infrastructures and more frequently leading to authorised push payments (APP) fraud. These techniques have greatly evolved over the last years as the targets are users rather than technology.
- Awareness campaigns are still very important countermeasures against social engineering, and these campaigns should be coordinated, involving also public administrations. They should target individual and corporate customers, as well as employees. Service providers can implement techniques helping customers to verify that websites and emails are genuine and can provide customers with authenticators which do not expose sensitive information. The service providers can also implement protection mechanisms in their email infrastructure and take benefit from specialised services for closing down phishing websites.
- Malware – existing in various forms - remains a major threat, in particular ransomware has been on the rise during the past year, requiring new mitigating measures.

- Measures against malware include proper maintenance of own devices by the customers, including mobile devices (regularly update the operating system, use only needed software, install and activate anti-virus and anti-malware tools, enable secure access, etc). Service providers' customer relations departments should inform their customers about these measures, and IT departments should implement adequate protection and control functions in their applications. Specific control and mitigation measures should also concern the usage of Cloud services by the PSPs.
- One of the most sophisticated and lucrative types of payment fraud now and for the future seems to be Advanced Persistent Threat (APT). It must be considered as a potential high risk not only for payment infrastructures but also for all network related payment ecosystems.
- Measures against APTs should start with security defense-in-depth strategy and architecture but must go beyond and include advanced security data analytics, technologies of early detection with real-time reporting and visualisation. Mechanisms to recognise APTs signs and patterns can also be effective.
- The number of DDoS attacks has increases and they are still frequently targeting the financial sector. There is a continuation of botnets and because of the high volume of infected consumer devices (e.g. PCs, mobile devices, etc.) severe threats remain. Extortion or ransom DDoS (RDDoS) attacks started to become a new threat.
- Against DDoS attacks, PSPs can set up a dynamic security control framework, implement services to filter fraudulent traffic and mitigating measures against application-level attacks. Testing the DDoS measures is also important, and this can include simulated attacks.
- Botnets can act as a force multiplier for malicious activity, including DDoS, using compromised systems from computers to IoT devices. Botnets are also a preferred means to mine crypto-currency drawing on the victim's system computing power and electricity.
- For combating botnet threats various technical countermeasures can be adopted but regulatory and social countermeasures such as cybercrime dedicated laws, user awareness and enhanced cooperation, are also important.
- Third-party vendors are more and more critical for PSPs and they can introduce new risks. Therefore, the management of relations with suppliers is of crucial importance in banking and financial legislation in order to prevent consequences such as data breaches, financial losses, and operational failures.
- A fraudulent payment transaction is often followed by the use of a monetisation channel such as an immediate cash withdrawal, a purchase with no trace, a money transfer or a transfer to another account ("money mulling").
- Raising awareness among customers, identification of "mules" combined with monitoring and stopping measures should be adopted as mitigation actions.

Attacks leading to fraud can occur in all *payment-relevant processes*: on-boarding/provisioning, Request-to-Pay/E-Invoicing, initiation/authentication and execution. Often attacks are caused by exploiting a combination of several threats. Appropriate countermeasures depending on the threat type should be adopted:

- At onboarding and provisioning stage, attacks can target client information in an authoritative registry (e.g. postal address, mobile telephone number), make use of stolen credentials, and notably using SIM swapping.

- Invoicing and Request-to-Pay stages are particularly exposed to APP fraud or IBAN manipulation, including tampering of QR-codes.
- Initiation and Authentication are primarily exposed to malware attacks. Such attacks can be combined with social engineering (e.g. the customer is informed that a specific payment has been initiated, a payment has been erroneously received and should be reimbursed, etc.)
- Attacks at the payment execution stage focus on processing systems where the actual validation of the transaction and transfer of funds is executed. The most relevant type of at this stage attacks are via DDoS and APTs.

If the perspective of the analysis shifts from the payment processes to *payment instruments and payment schemes*, the following specificities may be observed:

- Concerning card payment fraud, criminals are changing their approach. Not only by changing to more high-tech frauds like APT, but also a part of the criminals is reverting to old school types of fraud such as lost and stolen, sometimes in combination with social engineering. As e-commerce is still on the rise, CNP fraud remains a significant factor for fraud losses.
- For SEPA Credit Transfer (SCT) and Direct Debit (SDD) transactions, the criminals' use of impersonation and deception scams, as well as online attacks to compromise data, continue to be the primary factors behind fraud losses. Hereby criminals target personal and financial details which are used to facilitate fraudulent transactions. During the past year an increase in APP fraud is to be noted.
- For SEPA Instant Credit Transfer (SCT Inst), in addition to the threats targeting SEPA SCT, its specific features can be also exploited: immediate execution followed by immediate clearing and settlement with funds instantly made available to the beneficiary, and continuous processing on a 24/7 basis
- Supporting SEPA schemes (SPL and SRTP) are relatively new, meaning that it is too early to observe real-life fraud cases targeting them to draw any meaningful conclusions. It can be expected that the same patterns of threats and fraud enablers can affect them.
- Specific threats in the mobile wallet include targeted attacks on mobile device key stores, unlock credentials, user interfaces and NFC controllers.

Regardless the threats specific to particular schemes or payment processes, an important aspect to mitigate the risks and reduce the fraud is the sharing of fraud intelligence and information on incidents amongst PSPs.

This document is maintained by the Payment Security Support Group (PSSG), the EPC group of experts responsible for providing advice and guidance on security issues affecting payments or payment-related services within the framework of the EPC's activities.

It is also worthwhile mentioning that the EPC has established a group on fraud related to the SEPA payment instruments, namely the Payment Scheme Fraud Prevention Working Group (PSFPWG). The aim is to contribute to operational payment fraud prevention by facilitating SEPA payment scheme fraud data collection and analysis, information sharing and prevention measures.

Finally, PSPs must understand the emerging threats, the possible impacts and should keep investing in appropriate security and monitoring technologies as well as in customer awareness campaigns.

1 Document Information

1.1 Scope and Objectives

The present document aims to provide an insight in the latest developments on threats affecting payments, including cybercrime. It further provides an insight into the payments fraud resulting from criminal attacks. However, it does not endeavour to be a complete report on all criminal activities. It only attempts to create awareness on these matters to allow stakeholders involved in payments to decide on possible actions in this respect in order to maintain the trust in their payment solutions. Section 1 provides the references, definitions, and abbreviations used in this document. Section 2 sets out a relevant list of the most recent attacks. Section 3 covers a broader landscape of attacks: generic to payment processes and payment instruments, specific ones exploited nowadays against payment processes, and specific ones to payment instruments. The conclusions of this report may be found in Section 4. Annex I contains a summary of the threats and the main suggested controls and mitigation measures for each threat.

1.2 Audience

The document is intended for PSPs as well as for other interested parties involved in payments, such as:

- Third Party Service Providers
- Equipment manufacturers (POIs, consumer devices, etc.);
- Merchants and merchant organisations;
- Regulators;
- Standardisation and industry bodies;
- Payment schemes;
- Other interested stakeholders.

1.3 Contributors

Several EPC experts have participated in the development of this report over time. The contributors to the 2023 update are:

- Alain Hiltgen (UBS Business Solutions AG, Switzerland)
- Ioannis Tzanos (Eurobank, Greece)
- Laurens Messing (Dutch Banking Association, The Netherlands)
- Mika Linna (Finance Finland)
- Simone Coltellese (CERTFin, Italy)
- Valentim Oliveira (SIBS, Portugal)
- Valentin Vlad (EPC Secretariat)

1.4 References

This section lists the main references mentioned in this document. Square brackets throughout this document are used to refer to a document in the list. Other references are included as footnotes throughout the document.

Ref nr	Document	Author
[1]	Payment Services Directive (PSD2) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payments services in the internal market	EC

[2]	Commission Delegated Regulation (EU) 2018/189 of 27 November 2017 supplementing Directive (EU) 2015/2366 (PSD2) with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as "RTS")	EC
[3]	Network Information Security Directive (NIS Directive) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	EC
[4]	General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data	EC
[5]	EBA-Op-2019-11: Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions	EBA
[6]	Digital operational resilience act (DORA)	EC

Table 1 Bibliography

1.5 Definitions and Abbreviations

Throughout this document, the following terms are used.

Term	Definition
Authentication	The provision of assurance that a claimed characteristic of an entity is correct. The provision of assurance may be given by verifying an identity of a natural or legal person, device or process.
Authorised Push Payment scam (APP scam)	This is fraud caused by a criminal who tricks their victim into transferring money directly from their account to an account which the criminal controls, whereby the victim authorises the payment themselves.
Automated Teller Machine (ATM)	An unattended physical POI that has online capability, accepts PINs, which allows authorised users, typically using machine-readable plastic cards, to withdraw cash from their accounts and/or access other services (e.g., to make balance enquiries, transfer funds or deposit money).
Beneficiary	See Payee
Black Box attack	Connection of an unauthorised device which sends dispense commands directly to the ATM cash dispenser, in order to "cash-out" or "jackpot" the ATM.
Cardholder	A customer who has an agreement with an issuer for a card payment service.

Card Not Present (CNP)	A card transaction with no physical interaction between the card and a POI at the time of the transaction, also referred to as a remote card transaction.
Consumer	A natural person who, in payment service contracts covered by the PSD2, is acting for purposes other than his or her trade, business or profession (see [1]).
Contactless Technology	A radio frequency technology operating at very short ranges so that the user has to perform a voluntary gesture in order that a communication is initiated between two devices by approaching them. It is a (chip) card, customer mobile device or mobile payment acceptance technology at a POI device which is based on ISO/IEC 14443.
Customer	A payer or a beneficiary which may be either a consumer or a business (merchant or a corporate).
Credential(s)	Payment account related data that may include a code (e.g., mobile code), provided by the PSP to their customer for identification/authentication purposes.
Credit transfer	A payment instrument for crediting a payee's payment account with a payment transaction from a payer's payment account by the PSP which holds the payer's payment account, based on an instruction given by the payer (see [1]).
Digital wallet	A service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc.). A digital wallet is sometimes also referred to as an e-wallet.
Direct debit	A payment instrument for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's PSP or to the payer's own PSP (see [1]).
Dynamic authentication/linking	An authentication method that uses cryptography or other techniques to create a one-per-transaction random authenticator (a so-called "dynamic authenticator").
EMVCo	An LLC formed in 1999 by Europay International, MasterCard International and Visa International to enhance the EMV Integrated Circuit Card Specifications for Payments Systems. It manages, maintains, and enhances the EMV specifications jointly owned by the payment systems. It currently consists of American Express, Discover, JCB, MasterCard, Union Pay and VISA.
(Card) Acquirer	A PSP contracting with a payee to accept and process card-based payment transactions, which result in a transfer of funds to the payee.

(Card) Issuer	A PSP contracting to provide a payer with a payment instrument to initiate and process the payer's card-based payment transactions.
In-app payment	These are payments made directly from within a mobile application (e.g., a merchant app). The payment process is completed from within the app to enhance the consumer experience.
Instant Credit Transfer	A form of Credit Transfer available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account.
Merchant	The beneficiary within a mobile payment scheme for payment of the goods or services purchased by the consumer. The merchant is a customer of their PSP.
Mobile Network Operator (MNO)	A mobile phone operator that provides a range of mobile communication services, potentially including facilitation of NFC services. The MNO ensures connectivity Over the Air (OTA) between the consumer and their PSP using their own or leased network.
Mobile wallet	A digital wallet accessed through a mobile device. This service may reside on a mobile device owned by the customer (i.e. the holder of the wallet) or may be remotely hosted on a secured server (or a combination thereof) or on a merchant website. Typically, the so-called mobile wallet issuer provides the wallet functionalities, but the usage of the mobile wallet is under the control of the customer.
Near Field Communication (NFC)	A contactless protocol for cards and mobile devices specified by the NFC Forum for multi-market usage. NFC Forum specifications are based on ISO/IEC 18092 but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443.
Payee	A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction (see [1]).
Payer	A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order (see [1]). Note: In case of card-based payments this may also be referred to as cardholder.
Payment account	An account held in the name of one or more payment service users which is used for the execution of payment transactions (see [1]).
Payment scheme	A single set of rules, practices, standards and/or implementation guidelines for the execution of payment transactions and which is separated from any infrastructure or payment system that supports its operation, and includes any specific decision-making body, organisation or entity accountable for the functioning of the scheme.
Payment Service Provider (PSP)	A body referred to in Article 1(1) of [1] or a natural or legal person benefiting from an exemption pursuant to Articles 32 or 33 of [1].

Payment transaction	An act, initiated by the payer or on his behalf or by the payee (beneficiary), of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee (as defined in [1]).
Personal Identification Number (PIN)	A personal and confidential numerical code which the user of a payment instrument may need to use in order to verify their identity.
Point of Interaction (POI)	The initial point where data is read from a customer device or where consumer data is entered in the merchant's environment or ATM. As an electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a customer to perform a payment transaction.
Third Party Payment Service Provider (TPP)	A third party that offers payment services which are different to the Account Servicing PSP (ASPSP) such as a Payment Initiation Service Provider (PISP), Account Information Service Provider (AISP) and Trusted Party Payment Instrument Issuer (TPPII)
(Payment) Tokenisation	The usage of payment tokens instead of real payer related account data in payment transactions.
(Payment) Token	Payment Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for payer account related data (e.g., the PAN for card payments, the IBAN for SCTs). Payment Tokens must not have the same value as or conflict with the real payment account related data.

Table 2 Definitions

Throughout this document, the following abbreviations are used.

Abbreviation	Term
ACS	Access Control Server
3DS	EMV® 3-D Secure Specifications
APT	Advanced Persistent Threat
ATA	Advanced Targeted Attacks
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CSA	Cloud Security Alliance
CSDE	Council to Secure the Digital Economy
CSP	Cloud Service Provider
C-SCRM	Cyber Supply Chain Risk Management
CVV	Card Verification Value
C&C	Command and Control
DoS	Denial of Service

DDoS	Distributed Denial of Service
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DOTS	DdoS Open Threat Signalling
DVR	Digital Video Recorder
EBA	European Banking Authority
EC	European Commission
ENISA	European Network and Information Security Agency
EPC	European Payments Council
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HSTS	HTTP Strict Transport Security
IBAN	International Bank Account Number
IDS	Intrusion Defense System
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Preventions System
ISO	International Organization for Standardization
IT	Information Technology
MitM	Man-in-the-Middle
KYC	Know Your Customer
NIST	National Institute of Standards and Technology
OTP	One-Time Password/Passcode
OWASP	Open Web Application Security Project
OWASP MASVS	OWASP Mobile Application Security Verification Standard
PAN	Primary Account Number
PC	Personal Computer
SIEM	Security Information and Event Management
SIM	Subscriber Identification Module
SMS	Short Message Service
SPF	Sender Policy Framework

SWIFT	Society for Worldwide Interbank Financial Telecommunication
TPP	Third Party Payment Service Provider
URL	Uniform Resource Locator

Table 3 Abbreviations

2 Focus on recent attacks

This section sets out a relevant list of attacks s that have been recently observed by the communities represented in the EPC.

Social engineering attacks persist and are becoming more creative. Attackers often spoof phone numbers or SMS sender IDs to enhance the credibility of their tactics.

Malware attacks, particularly on mobile devices, are finding new ways to infect devices. This includes leveraging accessibility features, injecting malware into legitimate app updates, or distributing bogus apps.

Additionally, there has been a spread of ATM MitM and relay attacks to various European countries since last year.

- **Remote support scam**: These techniques could be combined with social engineering to deceive customers to call fake telephone numbers displayed as a result of a web search, as bank customer support numbers. When the customer calls this number a fake Microsoft support employee answers, who convinces the customer to install a remote support tool. This tool is use by the fraudster to take control of the customer device and continue fraudulent actions. One example is opening an account in a crypt-exchange platform in the name of the customer to transfer the "support fee" to this account.
- **New forms of smishing**: criminals use web tools for sending bulk SMSs including the bank name in the SMS text or as originator CallerID when this is possible, so spoofing the originator/genuine bank CallerID number is not anymore so necessary; or using short numbers used in the past. Also "spear phishing" via SMS has been observed, where the real name of the customer appears in the text of the SMS, in order to gain confidence. Other forms of smishing can lead the customers to websites cloning the bank website for collecting credentials and can be combined with fake support phone calls from the fraudsters guiding the victims to operations ending in full activation of the two-factor authentication on the fraudster's device.
- **"Save account"** fraud: using classic social engineering methods, the fraudsters convince customers that their account is at risk and they need to approve the transfer of money to a "safe" account, which actually is under the control of the fraudster.
- Fraud through **fake auction or e-commerce sites**. This is a simple modus operandi involving a payment by credit transfer for goods advertised on fake auction or e-commerce sites. The goods are obviously not delivered, and the money received are quickly withdrawn as cash using debit cards or transferred by accomplices located on other continents.
- Malware such as **"Banking Trojans", especially on mobile devices**. New features are being added to such malicious: remote control of the infected device, the interception of SMSs and the replacement of the beneficiary of a payment in real time. Other, even more sophisticated features have been also observed: ATS (Automated Transfer System) modules powered by Accessibility Service in order to scale on-device fraud attempts, Remote Access sessions (RAT) relying on Android native code or hiding malware directly on Google Play store (e.g. initially via legitimate applications but the malware is installed via updates) evading Google detections techniques.
- Malware delivered as malicious **SMS managers on mobile devices**, that are used to to gain access to two-factor authentication codes.

- **Interception of credit cards renewal letters**. The card is replaced by a counterfeit card and the letter contains instructions for phone activation, requesting the victim to provide the card number and the pin code.
- **"ATM MitM and relay attacks"**: The victim attempts to withdraw cash from an ATM unaware that the ATM is trapped with a shimmer so that chip card data are transmitted to a relay card inserted at a rogue ATM, and the PIN typing is being video streamed to an attacker that eventually types in the PIN and finally collects the bank notes on the rogue ATM.
- **"SEO poisoning"**, meaning the use of Search Engine Optimisation (SEO) techniques to trick customers by leading them to websites controlled by fraudsters who buy keywords from search engines in order to obtain higher rankings in the search results. The fake websites for example impersonating legitimate web banking websites are used by fraudsters to collect confidential data or login credentials. A variant of this pattern is when "typosquatting" domains (a common misspelling of another organisation's domain) are registered by fraudsters. These domains do not expose malicious content but clone pages of sites to search and compare mortgages and loans as legitimate content. However, the victims are redirected through these pages to real phishing pages.

3 Broader Attack Vector Landscape

3.1 Threats and other Fraud Enablers

3.1.1 Social Engineering

Social engineering is an attack vector that exploits human error to gain private information, access, or valuables. In social engineering, the attackers can employ a variety of techniques to manipulate unsuspecting customers, employees or third parties into exposing data, spreading malware infections, or giving access to restricted systems.

In a corporate context, social engineering attacks often seek to gather and exploit information about the target organisation's business processes, decision-making structures, and any underlying gaps of control deficiencies that could facilitate CEO fraud, business email compromise, or any other kind of business process fraud.

Social engineering attempts can take place online across many channels, including email, SMS, phone calls and social media, in-person, and via other interactions. Attackers often prefer social engineering over more technology-oriented attacks because they are scalable, inexpensive, and more difficult to attribute to a specific actor.

The goals of social engineering attacks vary. Social engineering may be used, first, to gain access to systems via tricking users into exposing their credentials (phishing) or uploading malware into their systems. Here, the attacker's possible objectives might include: the initiation of payments without the victim's consent (payment fraud) or the infection of the victim's systems with remote access malware – enabling persistent access to the target's systems and data – or with other type of malicious software, such as ransomware designed to encrypt the target's data for subsequent extortion purposes. Further information on different types of malware is provided in Sections 2.2.

However, social engineering may also be used to manipulate victims into initiating themselves payments to accounts controlled by the attacker (authorised push payment or APP scam). In addition to the CEO fraud and business email compromise mentioned above, APP scams include such as romance scams, purchase scams, investment scams, advance fee scams, and impersonation scams which are discussed in more detail in Section 3.3.

Social engineering attacks further range from mass email attempts that can be more or less easy to identify as an attempt to defraud a customer, to dedicated emails or voice calls that target a specific customer or employee (spear phishing).

Details on fraud caused by social engineering on payment-relevant processes and specific payment instruments, may be found in Sections 3 and 4.

3.1.1.1 Impact and Consequences

Social engineering techniques have greatly evolved over the last years as attackers increasingly target users rather than technology. All types of social engineering attacks continue to be used by attackers of varying levels of capabilities, with a particular increase in business email compromise and phishing emails that result in malware being deployed on computers.

Phishing plays a key role in carrying out targeted digital attacks. Some users are not able to recognise phishing emails. However, the implementation of DMARC by organisations to stop phishing emails have experienced a quite big take-up in some countries and have proven to be successful. Nevertheless, phishing continues to be a low-threshold and effective method for attackers.

Large scale phishing can be enabled by using Botnets as instruments for amplifying the extent and intensity of attacking campaigns. More details about botnets will be given in Section 2.5.

3.1.1.2 Suggested Controls and Mitigation

Awareness campaigns are still very important countermeasures against social engineering. Following are some examples of messages:

- "Never give away your personal data, password or OTPs to someone who calls."
- "Do not click on links on e-mails, directly visit the PSP website instead."
- "Double check any payment information received by e-mail with the legitimate sender by a different means."

It is important to denote that this advice is important, no matter who the caller or sender claims to be or how urgent the caller says it is.

The warning against phishing is simple, but to get the message through and enable customers to comply in stressed situations is not simple. PSPs need to have a proper customer education system in place, not only addressing individual clients but also including SMEs and large corporates, explaining the risks in layman words. In some countries coordinated campaigns are being set up where the financial industry cooperates with public or semi-public agencies. In addition, it is as important for companies and organisations (including PSPs) to also adequately educate and create awareness amongst their own staff.

The customer's possibility to determine whether an email or website is genuine should be supported by service providers by ensuring that:

- Login screens only occur in https sessions using certificates with Extended Validation.
- Websites consistently use the same easy-to-recognise domain names / URLs.
- Websites support HSTS.
- Emails to customers never contain links to login screens asking for passwords etc. or other sensitive information.

The sender of **phishing** emails will typically like to spoof the domain name of a PSP or other trustworthy entity. Such organisations may try to prevent this by implementing the following countermeasures:

- Sender Policy Framework (SPF), which is an email-validation system designed to detect email spoofing.
- Domain Keys Identified Mail (DKIM)[1], which is an email authentication method designed to detect email spoofing by providing receiving mail exchangers to check that the incoming mail from a domain is authorised to be sent by that domain's administrators.
- Domain-based Message Authentication, Reporting and Conformance (DMARC)[2] which is an email-validation system designed to detect and prevent email spoofing. DMARC is built on top of the existing mechanisms mentioned before, SPF and DKIM and enables the blocking of spoofed mails.

[1] see for instance: https://www.gov.uk/government/publications/email-security-standards/domainkeys-identified-mail-dkim

[2] see for instance: https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc

An inherent countermeasure against phishing is to provide the user/customer with an authenticator, which does not expose any information of the user. Hence, the user cannot expose any credentials, but social engineering may still be used to trick the user in unintentionally authorising third-party access.

Private companies – working in close cooperation with telecom operators – offer takedown of phishing websites as a service. Such companies might be able to limit access to and finally stop phishing sites. In addition, it might also be possible sometimes to collect stolen data from phishing servers. The victim's PSP might then be able to reduce the consequences by contacting the customer and blocking the card or compromised authenticator.

3.1.2 Malware

Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software. Cybercriminals design malware to compromise computing functions, to steal data, to bypass access controls, and to cause harm to host computers, customer devices and their applications or data.

One of the major threats against cyber security today is malware. Malware comes in a wide range of flavours, such as viruses, worms, remote access tools, rootkits, Trojans, spyware and adware. Malware exploits software vulnerabilities in browsers, third party software and operating systems to gain access to the device and its information and resources. To spread, malware uses also social engineering techniques to trick users into installing and running the malicious code**.**

- ***Trojan horse*** – It is maybe the largest category of the malware family. It consists of a large variety of exotic names. However, they all have one thing in common; they bypass the security measure on the system to infect it. Their main purpose is stealing valuable information from the system and gaining control of the system itself. Trojans are also used to get an initial foothold and download other malware.
- ***Spyware, Adware & Banking Trojans –*** Spyware and adware, which are categorised as malware, are less dangerous for the users. Spyware is often classified into the following categories, *browser hijackers, tracking cookies* and *system monitors* (key-logging, take screenshots, record voice). In some cases *adware* is seen as the fourth category of spyware. These types of malware are all trying to track and store the usage and behaviour of users, serving them with pop-up ads when connected to the Internet. Based on the same approach, attackers are installing malware (Banking Trojan) targeting the victim while using e- or m-banking services. Banking Trojans are capable of hijacking the browser and tampering financial transactions or stealing user credentials during the use of e- or m-banking services. Banking Trojan can also be sent through weaponised attachments in an e-mail or infected software.
- ***Ransomware*** – Is a type of malicious software designed to encrypt files on the device or deny access to the device, which is the reason for it to be also known as cryptoware. It holds data up for ransom, blackmailing the user to pay a ransom to get back their data or access to their device. A surprising fact is that this kind of attacks seems to be more profitable to the attackers than the traditional banking Trojans.
- ***Remote Access Trojans (RATs)*** – A Remote Access Trojan is a piece of malware that allows a remote actor to control a system as if they have physical access to it. Use of a RAT may provide cybercriminals with unlimited access to the victims' computers. Using the victim's access privileges, the RAT can perform critical functions or steal sensitive data. RAT technology is also commonly used by APTs (see Section 2.3) to bypass strong authentication and get access to important data.

- ***RATs for Mobile*** – More recently RATs like Vultur[3] have surfaced also in the mobile space, exploiting Android's accessibility services in combination with standard remote access functionality. By leveraging a dropper or tricking the user in installing such an app and granting it accessibility rights, fraudsters get full remote control over the mobile's user interfaces, i.e., can easily spy on input/output to gather credentials but can also easily reinject captured data or push buttons upon request by a specific service or authentication app they would like to remote control. No mobile rooting is required for this to work.
- ***Fileless malware (also known as non-malware)*** – Fileless malware is a malicious code that does not need a file or script in order to operate. It takes advantage of existing vulnerabilities of the Operating System. It exists exclusively in a computer's RAM and uses system tools to inject malicious code into trusted processes. It is more difficult to prevent, detect and remove, as it does not leave a file for an antivirus software to detect. Hackers can steal data or install other forms of malware to give it persistence or hide it in some other trusted processes or internal persistent data. This way, it can set up scripts that run when the system restarts to continue the attack.

As organisations continue to migrate on-premises services and applications to the cloud or to externalise them to third parties, it is reasonable to deduce that these external resources will also suffer fraud threats and risks. Therefore, they become new targets of exposure to malwares and APTs.

3.1.2.1 Impact and Consequences

Whether the infection is targeting a private user, an SME or a multinational company the effects of a successful malware attack can cause significant damage, and every prevention and mitigating method should be utilised.

As an example, in May 2017 the WannaCry[4] ransomware malware strain gained infamy by crippling entire networks, across more than 150 countries, with hundreds of thousands of Windows computers infected.

In the case of PSPs, all necessary steps to prevent ransomware attacks should be taken. Ransomware attacks could involve encrypting of payment information, PANs and other information necessary for PSP business execution.

Ransomware has typically no impact on the users' banking credentials. Instead, by making use of banking Trojans, fraudsters have managed to extort a significant amount of money from users.

For private users spyware and adware are a large threat towards their privacy, as this type of malware looks for patterns of the users and tries to profile their individual behaviour for monetisation purposes. Similar things might happen for companies, but normally this type of malware targets individual behaviour, in fact it is their goal to group the individual by their own definitions, it is therefore not a direct threat towards corporate users.

Malwares normally search the infected machine for all information that can be monetised; for private users this is typically credentials related to e- or m-banking (mobile and web). Credit card credentials are of similarly high value. For private users the amount of information that can be sold to other parties is relatively small. Such information is easier to find in companies as each company retains databases of customer information or intellectual property, information which

[3] https://arstechnica.com/gadgets/2021/07/new-bank-fraud-malware-called-vultur-infects-thousands-of-devices/

[4] https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

can be used to blackmail or to give an advance in a competitive market. The above case has a significant impact in larger organisations or even governmental organisations where information is one of the most valuable assets.

3.1.2.2 Suggested Controls and Mitigation

User Controls and Mitigation

To prevent malware attacks, users should

- First minimise the number of installed programs on their device (and from trusted resources only), as the number of vulnerabilities will decrease accordingly.
- Secondly, one of the best ways to ensure that the system or device do not become infected with malware is to regularly update the installed software – especially the Operating System, which often release new versions to mitigate newly found vulnerabilities– and to remove software that does no longer have any use.
- An advice would however be to utilise specialised software to remove and protect against adware, as the latter also could use resources on the computer.

Related specifically to Mobile devices, users should implement some measures to mitigate the threats related to mobile devices, these include:

- Update the software running on your mobile device with the latest security patches and upgrades, these should be sent to you by your network / operating system provider.
- Use a secure lock screen, set a password, PIN or fingerprint to unlock your device.
- Do not allow applications to be installed from unknown / untrusted sources.
- Do not jailbreak or root your devices.
- Add a PIN or passcode to the voicemail on your mobile device.
- Do not use a PIN code which is your date of birth or which is part of an otherwise well-known information.
- Install anti-virus software on your mobile device.

PSP Controls and Mitigation

PSPs' departments dealing with customer relations should use every opportunity to inform their customers that it is very important to keep their software updated, and hence reduce the risk for malware infection significantly.

Mobile payment service providers should:

- Create awareness campaigns to educate consumers on how to avoid the previous explained fraud scenarios;
- Monitor app stores and Internet for fake applications;
- Implement anti-tampering and integrity controls in app;
- Associate jailbroken or rooted devices with a higher fraud score;
- Protect app code with code signing and obfuscation;
- Implement strong sensitive data encryption on device;
- Perform application penetration testing;
- Do not consider frequently used third-party libraries as secure and validate them before using them;

- Implement controls to protect communication channel (such as certificate pinning) to ensure an app will only communicate with a trusted party;
- Implement app as personalised and prevent transfer of personalised app to another device;
- Implement device owner/user verification as well as mobile device verification;
- Use always two-factor authentication, which should be implemented in a user-friendly way;
- Establish secure mobile payment app enrolment procedures, which cannot be circumvented by vishing and/or other social engineering scams;
- Check vulnerabilities based on the OWASP MASVS list.

Service Providers or PSP IT departments Controls and Mitigation

Service providers' or PSPs' internal IT departments should implement measures such as:

- Script blockers, so that the device becomes less exposed to the risk, and therefore the risks of infections are smaller.
- All critical files should be regularly backed up so that they can be recovered in the case of unauthorised alteration, encryption, or destruction.
- Monitoring of files/software (executables) behaviour can help to block certain threats such as ransomware. This is generally referred to as "malware behaviour blocking".
- Limited use of administrative rights; this is mostly applied by companies and security aware users, as most users would not see the benefit of it in their everyday needs. Firewall and antivirus on consumer devices should be regularly updated. It is also strongly recommended to enable further controls provided by the endpoint security mechanisms, such as the IPS/IDS capability on the device[5], when applicable.
- Ensure that macros cannot run on the systems while opening attachments or documents in general. This is typically the case for most large companies, however smaller companies and private users largely depend on the patches that are automatically installed by the office suite software provider as they do not understand the threat. Allowing the execution of only signed macros can be the solution to securely exclude malware without losing functionality or breaking business needs.
- Consider the use of Web isolation technologies in order to let potential threats run in a secure environment (sandbox).

Controls and Mitigation specific for the usage of Cloud services

Before using a cloud service, a PSP must identify assets (data, applications, infrastructure) and evaluate them (criticality, classification) and define the appropriate security controls. Then they should choose an appropriate cloud deployment model and define whether and how the data can move in and out of the cloud. Finally, there should be a due-diligence process to evaluate the service provider regarding security, privacy, availability and their SLA.

[5] Intrusion Prevention Systems / Intrusion Defense Systems are security mechanisms deployed on servers or devices which monitor in real-time for entries representing a security violation. Some common abilities of such mechanisms include integrity checking, policy enforcement, rootkit detection, detection of variations in system configuration. They offer the ability to identify intrusion attempts and actively prevent malicious or anomaly activity on the host system. IPS/IDS could be deployed at the network level too.

- Cloud governance including a risk-based analysis approach, based on international standards such as NIST, ISO 2700x, COBIT or PCI-DSS as well as continuous monitoring of the implemented controls are first steps to mitigating or reducing the fraud risks.
- Of equal importance is the regular execution of a security audit to verify the cloud provider's conformity to the security requirements through the whole lifecycle of the application.
- PSPs must always have the control over their data, security included. For example, when encryption is used for data privacy, PSPs must have control over the key management and not the cloud provider. Also, where technically possible, the authentication mechanism should always be controlled by the company and not by the cloud provider.

Controls and Mitigation for the usage of multi-purpose authentication means

Multi-purpose authentication means, as exemplified by the currently developed EUDI-Wallet[6], confront a different form of exposure not encountered by authentication means dedicated to a specific purpose (e.g. an online banking service from a specific PSP). Malware could trick end-users into granting authorization for the use of their securely guarded credentials, ostensibly for an uncritical activity (e.g. accessing an exclusive shopping opportunity), while effectively misusing these authorized credentials for illicit access to the end-user's online banking account. This exposure notably exists irrespective of the level of credential protections (e.g. hardware keystore, strong biometric access) generally implemented to protect against credential theft or unauthorized usage. To counter this threat:

- Multi-purpose authentication means must incorporate a secure execution environment that supports authentication with linking through a trusted user interface. Such feature is necessary to effectively confine an end-user's authentication to a service that can be clearly displayed and agreed upon by the end-user.
- For PSPs that support multi-purpose authentication means for the access to their online banking services it is imperative that they grant access only when they can unequivocally verify, via a robust linking mechanism, that the utilization of the multi-purpose authentication means was genuinely authorized by the end-user for access to their specific service.

3.1.3 Advanced Persistent Threats (APT)

An Advanced Persistent Threat is a sophisticated, targeted, malicious attack aimed at a specific individual, company, system or software, based on some specific knowledge regarding the target. It pursues its objectives repeatedly over an extended period of time, adapts to defenders' efforts to resist and is determined to maintain the level of interaction needed to execute its objectives[7].

The term APT originated in the U.S. Department of Defense late in the first decade of the 21st century to describe cyberespionage efforts by China against American national security interests.[8]

APTs are different from other targeted attacks in the following ways:

---

[6] https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

[7] National Institute of Standards and Technology (NIST), Special Publication 800-39, Managing Information Security Risk, Organization, Mission, and Information System View, USA, 2011

[8] https://www.britannica.com/topic/advanced-persistent-threat

- **Customised attacks** – In addition to more common attack methods, APTs often use highly customised tools and intrusion techniques, developed specifically for the campaign. These tools include zero-day vulnerability exploits, viruses, worms, and rootkits. In addition, APTs often launch multiple threats or "kill chains" simultaneously to breach their targets and ensure ongoing access to targeted systems, sometimes including a "sacrificial" threat to trick the target into thinking the attack has been successfully repelled.
- **Low and slow** – APT attacks occur over long periods of time during which the attackers move slowly and quietly to avoid detection.
- **Higher aspirations** – Unlike the fast-money schemes typical for more common targeted attacks, APTs are designed to satisfy the requirements of international espionage and/or sabotage, usually involving covert state actors. The groups behind APTs are well funded and staffed; they may operate with the support of military or state intelligence.
- **Specific targets** – Widely reported APT attacks have been launched at government agencies and facilities, defense contractors, and manufacturers of products that are highly competitive on global markets. In addition, APTs may attack vendor or partner organisations that do business with their primary targets. Ordinary companies with valuable technology or intellectual property and financial institutions managing their clients' valuable assets are now being targeted by nation states.

APTs can often be seen as an outstanding category of malware. Attackers demonstrate a continuously improving set of skills, in bypassing security mechanisms, providing often a state-of-the-art attack that changes the roadmap and trends of the security industry. This is also known as zero-day attacks, since no normal signatures exist from the antivirus / antimalware tools.

The APT attacks are often executed following a structured approach. Experts have identified typical stages of an attack starting with the selection of the target, going through the information gathering, gaining access to the target, exploitation and operation, and terminating with data discovery, collection and exfiltration.[9]

APT attacks can further be recognised by special signs that hackers leave behind. Over the past two decades, Roger Grimes discovered the following five signs most likely to indicate that a company has been compromised by an APT[10]:

- *Increase in elevated logons late at night*
- *Widespread backdoor Trojans*
- *Unexpected information flows*
- *Unexpected data bundles*
- *Focused spear-phishing campaigns*

APT attacks may target financial institutions with the aim to compromise the network or payment system e.g., to perform unauthorised transactions and steal money.

More details on fraud caused by APT on payment processes and specific payment instruments, may be found in the Section 3 and 4.

[9] ¡

[10] https://www.csoonline.com/article/2615666/security/security-5-signs-you-ve-been-hit-with-an-advanced-persistent-threat.html Parts of this article are presented verbatim above.

3.1.3.1 Impact and Consequences

The APT's single-minded persistence on pursuing its target and repeated efforts to complete the job for which it has been created with malicious intent, makes that the attack will not go away after one failed attempt. It will continually attempt to penetrate the desired target until it meets its objective.

In recent years not only criminal but also state organised APT attacks have been seen around the globe, targeting financial institutions. Although parties like Europol and Interpol have done proper jobs with arresting gang members, criminal organisations such as Cobalt and Carbanak have been very active in 2018 attacking financial institutions. Modus operandi from these gangs varies by doing field research on the financial institutions to spear phishing on staff members with email infected with malware.

The Global Research and Analysis Team (GreAT) at Kaspersky reported last July the following trends[11]:

- The discovery of the long-running Operation Triangulation campaign, including the previously unknown iOS malware platform.
- Established threat actors enhancing their toolsets over time. So far, in 2023 has been no different – in particular, this includes Lazarus's development of its MATA framework, the new delivery methods and programming languages used by BlueNoroff, new infection methods used by ScarCruft and new malware samples from GoldenJackal.
- A campaign from the newly discovered threat actor Mysterious Elephant.
- Threat actors using a variety of different programming languages.
- APT campaigns continue to be geographically dispersed. In 2023 actors have been focusing their attacks on Europe, Latin America, the Middle East and various parts of Asia.
- Geopolitics remains a key driver of APT development, and cyber-espionage continues to be a prime goal of APT campaigns.

APT38, which has been active since 2014, is a financially motivated group linked to North Korean cyber espionage operators, renowned for its attempt to steal hundreds of millions of dollars from financial institutions through the brazen use of destructive malware. APT38 executes sophisticated bank heists that typically feature long planning, extended periods of access to victim environments preceding any attempts to steal money, fluency across mixed operating systems, the use of custom developed tools and constant effort to thwart investigations capped with a willingness to destroy compromised machines. APT38 has compromised more than 16 organisations in at least 13 different countries, sometimes simultaneously, since at least 2014. Victimised organisations tend to be in developing economic regions. Although APT38 focuses almost exclusively on the financial sector, its bank heists are reminiscent of sophisticated espionage campaigns. APT38 continues to conduct phishing activity against Bitcoin and other cryptocurrency-related financial services.

[11] https://www.kaspersky.com/about/press-releases/2023_kaspersky-unveils-latest-apt-trends-for-q2

Blue Mockingbird[12] is a cluster of observed activity involving Monero cryptocurrency-mining payloads in dynamic-link library (DLL) form on Windows systems. The earliest observed Blue Mockingbird tools were created in December 2019. They achieve initial access by exploiting public-facing web applications, specifically those that use Telerik UI for ASP.NET, followed by execution and persistence using multiple techniques. During at least one incident, the adversary used proxying software and experimented with different kinds of reverse shell payloads to connect to external systems. As with other adversaries that mine cryptocurrency opportunistically, Blue Mockingbird likes to move laterally and distribute mining payloads across an enterprise. We observed Blue Mockingbird move laterally using a combination of the Remote Desktop Protocol to access privileged systems and Windows Explorer to then distribute payloads to remote systems

GootKit is a notable APT[13] example for its evasiveness and the stealthy way it steals confidential data and sends it back to the operators of its Command and Control (C&C) server. Primarily targeting European bank account holders, the malware has been known to capture videos of victims' desktops and dynamically inject fraudulent web content into the browsing sessions of users when they attempt to access their banking websites. To prevent detection by security tools, it checks for the presence of virtual machines that may be used by cybersecurity researchers to study the malware's behaviour.

3.1.3.2 Suggested Controls and Mitigation

APT is deemed a serious threat because of its nature to stay undetected for a long duration. APT malware is designed to evade detection from conventional perimeter security defenses (firewalls, IDS, IPS, endpoint protection platforms and secure Web gateways) used by most organisations. APT mitigation and detection capabilities need to be incorporated in a security defense-in-depth strategy and architecture, to protect enterprises from attacks of this complexity. The traditional defense-in-depth components are still necessary but are no longer sufficient in protecting against advanced targeted attacks and advanced malware.

Clearly, no single security control is able to provide effective, efficient protection, states Gartner, an IT research and advisory firm, noting that Advanced Targeted Attacks (ATAs) and advanced malware continue to plague enterprises. An APT defiance strategy needs to include real-time advanced security data analytics that can identify patterns of invasive behaviour and threat intelligence for detection-remediation-prosecution or attribution to stop attacks during an early stage.

Today's APTs are well coordinated, organised, and methodical, which makes them particularly difficult to detect by network security administrators, as many APTs use custom-developed code and/or target zero-day vulnerabilities. Nonetheless, by using technologies of early detection with real-time reporting and visualisation, network security administrators can try to perceive penetration as it happens before it disappears through the components of the system. Also, incorporating security threat intelligence into infrastructures and utilising best-practice mechanisms and procedures may help find the malware carefully hidden by cybercriminals inside enterprise networks.

---

[12] Blue Mockingbird, Group G0108 | MITRE ATT&CK®

[13] See e.g. https://www.sentinelone.com/blog/gootkit-banking-trojan-deep-dive-anti-analysis-features/

To confront such cyber-attacks will require system users to evaluate weak links in their infrastructure and employ defence controls that may recognise signs that something appears out of place. IT security managers need to look for patterns of events characteristic of APT methodologies. There are many proposed methods for mitigating APT, a few common methods not in order of effectiveness are highlighted in the following table:

No.	Mitigation Techniques
1	Traffic/ Data analysis
2	Pattern Recognition
3	Anomaly Detection
4	Awareness
5	Whitelists
6	Cryptography
7	Multi-layer security
8	Blacklists
9	Deception
10	SIEM
11	Intrusion Detection System (IDS)
12	Risk assessment

Table 4 Overview mitigation techniques used against APT attacks

Tools such as a SIEM solution try through security logs to detect any unauthorised or suspicious object access, or else OSSEC[14] and honeypots can detect host-based attacks on computers and allow early detection of APT behaviour. Also, they can find any cyber-attacks that bypass signature-based tools and common sandboxes.

Turning the table on attackers, deception technology lures attackers into attacking fake servers, services and many other networked IT resources that are found in the typical enterprise network. When attackers waste time and energy attempting to exfiltrate valuable data, security researchers gather valuable information about the methods they use, including insights into an attacker's kill chain, and adjust their network defenses accordingly.

To be able to effectively defend against today's new breed of cyber adversaries, and be able to counter APT and protect data from inappropriate access, it requires – apart from taking standard security countermeasures e.g. security hardening and patching of systems, and minimising the attack surface – strengthening existing authentication flaws (password weaknesses) and properly utilising proprietary security hardware/software. An advanced IP scanner application, for example, can help clean any form of malware, including spyware; whereas an APT scanner device that focuses on the detection of attacker activity can be of use should antivirus software and firewalls fail.

Furthermore, to test existing defenses and prepare advanced security preparedness, security professionals use the Red Team / Blue Team approach (used also by the military to test force-readiness) to identify vulnerabilities as part of the offensive attack activities, determine areas for improvement in the defensive incident response processes, identify opportunities to improve prevention and detection capabilities and develop response and remediation activities to return the IT landscape to a secure status. The Red Team is an independent internal or third-party group that assesses the organisation security readiness, tests active controls and countermeasures within a given operational environment and validate security defenses as well as the ability of

[14] https://www.ossec.net/

internal security resources to detect and respond to advanced security threats. The Blue Team consists of internal security resources with the mission to defend the operating environment against real or simulated cyberattacks over a significant period of time by the Red Team. This is accomplished by emulating the behaviours and techniques of likely attackers in the most realistic way possible. Based on the simulation findings, recommendations are provided to increase the organisation's cybersecurity readiness posture.

To support the cybersecurity professionals in their fight against Advanced Targeted Attacks, known as ATAs, Gartner has developed the Five Styles of Advanced Threat Defense Framework[15]. These styles are: network traffic analysis, network forensics, payload analysis, endpoint behaviour analysis, endpoint forensics, and can be used in combinations for a more effective approach.

3.1.4 Distributed Denial of Service (DdoS)

Distributed Denial of Service, or DdoS, involves crippling the systems of an organization usually customer facing websites by flooding the website systems with large amounts of malicious digital traffic. These attacks are usually carried out by low tier threat actors as they are widely available for purchase on the internet dark web. Although the impact on the stability of a targeted financial institution is limited, it can result in reputational damage for the institution and/or may hinder customer service. DdoS is deployed by actors across the entire actor spectrum, ranging from a script kiddy using a DdoS attack, to advanced threat actors using DdoS as a smoke screen for other stages of their attack.

DdoS attacks are one of the oldest internet cyberweapons used today by everyone from hacktivists and governments to disgruntled video game players and thrill-seekers purely for personal enjoyment. At the end of the last century, DdoS attacks were performed as a form of vandalism and without a clear strategy. This changed at the beginning of this century, and DdoS attacks now have specific objectives. They are used, for instance, to blackmail organisations for money or to protest against a country or organisation based on ideological motives. DdoS attacks are more and more often a modern form of protest. The attacks disrupt access to web sites and servers or take them offline completely by using co-opted online resources such as zombie PCs and servers or Internet of Things (IoT) bot networks that flood and overwhelm victims with online traffic. DdoS attacks are performed by many – sometimes hundreds of thousands – nodes at the same time, grouped in "botnets". In 2016 malware was released to incorporate IoT (Internet of Things) devices in DdoS botnets. IoT will dramatically increase the number of connected devices which are poorly patched. Therefore, IoT could give DdoS attackers an unpreceded DdoS bandwidth.

The ease for criminals, "script kiddies", etc. to prepare and execute a DoS attack is increasing. It is relatively easy and not expensive to buy or rent attack capabilities on the Internet. Two categories of perpetrators may be distinguished: "old school hackers" or "hacktivists" who just want to have a name or defend an ideology and the "hackers that essentially pursue financial gain". The latter ones use all means, human or technical failure, available to create blackmail or massive fraud. Moreover, DoS attacks are also used to conceal other attacks and distract the defenders.

DdoS attacks have been steadily increasing in frequency over the past few years. In its annual Distributed Denial of Service (DdoS) Insights Report[16], which analysed DdoS attack activity and its impact across industries in the first half of 2023, Zayo Group Holdings, Inc. found that DdoS attacks in the first part of 2023 were up 200% from 2022. Activity had increased nearly four-fold

[15] https://www.gartner.com/en/documents/2576720/five-styles-of-advanced-threat-defense

[16] https://go.zayo.com/resources/truth-and-trends-of-ddos-attacks/

from Q1 to Q2 in 2023 which Zayo insinuates has been caused by increased automation in the digital world. In a world of increasing digitisation, political unrest and the emergence of widespread hybrid/remote working patterns, the need for stringent cybersecurity measures has never been more urgent. Zayo states that these have all contributed to an increase in DdoS attacks.

Zayo highlights that DdoS has fast become the most common cyberattack against an organisation's online presence. They are deliberate attacks where a target's Internet is flooded with fake or illegitimate traffic to prevent true user traffic from passing. The scale of these attacks often cause hours of downtime, resulting in immense costs for businesses, including lost money, time, customers and reputation. These types of attacks also have the potential to severely impact key infrastructure and citizens.

Furthermore in is 11th annual ENISA Threat Landscape (ETL) report[17] ENISA (European Union Agency for Cybersecurity) stated that DdoS attacks are getting larger and more complex, are moving towards mobile networks and IoT and are being used in the context of being used in support of additional means in the context of a conflict.

"

Distinction can be made between four basic types of DdoS attacks:

- ***The flooding attack*** – The term 'flood' is a collective term used to describe the most basic form of DdoS attacks, namely those attacks that focus on making it impossible to gain access to a system or service, by exceeding the maximum bandwidth available. Exceeding the maximum available bandwidth means there is not enough bandwidth left for the legitimate data traffic.
  A special form of a flooding attack is the so-called amplification attack, for example a DNS-amplification attack. In an DNS-amplification attack, the attacker spoofs look-up requests to domain name system (DNS) servers to hide the source of the exploit and direct the response to the target. Through various techniques, the attacker turns a small DNS query into a much larger payload directed at the target network.
  The size of attacks is increasing caused by the number of infected end points. Moreover, the possibility to increase the size of an attack by combining it with an amplification attack is worrying.
- ***The protocol attack*** – Another way of causing a DdoS attack is to send data packets that take advantage of weaknesses in the communication protocols and other protocols used mainly by network devices such as routers and firewalls. These devices receive packets for processing that lead to unexpected results. For example, a large number of communication sessions are opened without being properly closed in due time, this way consuming the resources of the network device. As a result, they can no longer accept any new sessions. Well-known examples of protocol-attacks are SYN floods, fragmented packet attacks, Ping of Death and Smurf-attacks. The number of SYN-flooding attacks is increasing. In many cases the botnets used contain so called Internet of Things (IoT) devices. Examples of these devices are consumer electronics like home-routers, IP-cameras and smart-TV's. There are a lot of these devices nowadays and most of them are badly administered, resulting in non-patched systems and default administrator credentials.

[17] ENISA Threat Landscape 2023 — ENISA (europa.eu)

- ***The application-layer attack –*** An application layer DdoS attack is named after the OSI-layers' Application Layer (layer 7). The attacker is aiming at a specific function of a layer 7 protocol like http and misuses that function to exhaust the service. An example is the misuse of the GET/POST-function of http, performing a so-called slow attack which causes the web server to wait for a long time before answering the request of a web browser. An attack is disguised to look like legitimate traffic, except that it targets a specific function of the protocol it attacks. There is often not much bandwidth consumed and the e.g. web server just crashes. Application-layer attacks cannot be recognised as a DoS-attack during the encrypted transport. Only after decryption an application-layer attack can be recognised and mitigated.
- ***Combined attacks –*** At present combined attacks are becoming more frequent, using for example floodings and application-layer attacks at the same time, making mitigation of the attacks more complex.

DdoS attacks can also be used as an extortion-scheme. In this case, the victim receives an e-mail from an attack group asking for a (large) sum of money to prevent a (much larger) DdoS attack. Sometimes the email is preceded by the DdoS, as a proof of competence. The extortion message often refers to 'vivid' scenarios that are attributed to this offender group.

3.1.4.1 Impact and Consequences

Lately there has been a number of very large-scale attacks on non-PSPs.. Amazon said in February 2020 its online cloud, which provides the infrastructure on which many websites rely, has fended off the largest DdoS attack in history. Amazon Web Services (AWS) said the February attack had fired 2.3Tbps. The previous record, set in 2018, was 1.7Tbps[18]. Attackers pick up the pace and raise the bar. In 2021 alone, Akamai [19]saw more attacks over 50 Gbps (as of 03/24/2021) than were seen in all of 2019. Keep in mind attacks of this scale can take almost anyone offline. DdoS attacks are getting bolder and badder. Three of the six biggest volumetric DdoS attacks that have ever been recorded and mitigated have been in the first quarter in 2021, including the two largest known DdoS extortion attacks to date. Some of the latest attacks targeted an organization in Europe in the gambling industry and an organization in Asia in the video games industry. On Thursday, July 21, 2022, Akamai detected and mitigated the largest DdoS attack ever launched against a European customer on the Prolexic platform, with globally distributed attack traffic peaking at 853.7 Gbps and 659.6 Mpps over 14 hours. The attack, which targeted a swath of customer IP addresses, formed the largest global horizontal attack ever mitigated on the Prolexic platform[20].

The number of attacks in Q4 2021 increased by 52% against the previous quarter and more than 4.5 times against the same period last year. The numbers look scary, but instead of rushing to conclusions, better to figure out why they are so. Both of these factors — seasonal fluctuations and falling cryptocurrency prices — buoyed the DdoS attack market throughout Q4, hence the 1.5-fold increase. This becomes even clearer when viewing the stats by month: October accounted for 16% of all DdoS attacks in Q4, November 46% and December 38%, according to Kaspersky[21].

According to Securelist by Kaspersky, there has been an increase in DdoS attacks on VoIP providers. In early October 2021, British company VoIP Unlimited fell victim again, having been attacked by DdoS extortionists last quarter. The new wave of junk traffic was accompanied by a ransom demand. Similar attacks affected various other British providers. And in November, clients of VoIP provider Telnyx worldwide were hit by outages. The perpetrators could be the Revil group, which is linked to past attacks on VoIP providers and was liquidated by Russian law enforcement agencies in January, after the US authorities had supplied information about the attackers.

When people think of DdoS attacks, they focus on the outliers, the massive Terabit attacks that generate headlines. But the smaller, more focused attacks can do just as much damage. More importantly, these smaller attacks are actually more common than their larger-scale counterparts. Sometimes, criminals will attempt credential stuffing attacks side by side with distractions, such as DdoS attacks, or they will skip the credentials and attempt to exploit applications or website vulnerabilities on the target's domain.

DdoS attacks are a problem for any organization, but they are especially a problem for the financial services industry. The financial services sector is still a prime target for cyber criminals. According to Boston Consulting Group research, financial service firms are up to 300 times more likely to experience a cyber-attack per year compared to companies in other industries. With the global pandemic and remote working driving significant increases in DdoS attacks on financial

[18] https://www.bbc.com/news/technology-53093611

[19] Akamai Blog | 2021: Volumetric DDoS Attacks Rising Fast

[20] Akamai Blog | 2021: Largest European DDoS Attack on Record

[21] https://securelist.com/ddos-attacks-in-q4-2021/105784/

services in the first half of 2020 this appears to be a trend that is set to continue[22]. A successful DdoS in the financial world could mean millions of euros lost for each minute of downtime. As mentioned, sometimes criminals will launch DdoS attacks as a distraction, either to conduct credential stuffing attacks or to exploit a web-based vulnerability. Banking, financial services and insurance (BFSI) was the industry most targeted by DdoS attacks in 2021[23], subjected to more than a quarter of the total volume. That continued a trend which has seen attacks against BSFI steadily rising since the beginning of 2020. By contrast, technology, the most targeted sector of 2020, fell into fourth place behind telecommunications and education. Between them, these four industries accounted for 75% of all recorded attacks, with a long tail of others including energy, retail, healthcare, transportation and legal that saw hardly any adverse activity.

The potential impact of a DDoS attack is twofold. On the one hand it can lead to the temporary unavailability of a PSP, including all its services, e.g. Internet banking, mobile banking, but also non-payment related services. And that can again lead to a form of blackmail (see next paragraph) by the attacker and/or – caused by a focus of many on re-establishing the service – a potential increase in successful fraud attempts. On the other hand, a consequence can be damage to the reputation of the attacked PSP, where e.g. the Internet banking service is “again” not available.

A group calling themselves "Cozy Bear" has been emailing various companies with an extortion letter, demanding payment and threatening targeted DdoS attacks if their demands are not met. Cozy Bear, also known as APT29, is known for its customized malware and attacks on commercial entities and government organizations across the globe. Akamai believes the letter is from a copycat group leveraging the Cozy Bear name as a means to invoke fear and panic. Their extortion letter actually suggests victims perform a Google search on their name, which immediately returns results related to the infamous group. So far, multiple companies have reported receiving an email demanding a sum of about $17,500 in Bitcoin, or 2 BTC, at the time this advisory was written. If the payments are not made before the deadline expires (usually 6 days), the price increases by 1 BTC each day the demand is not met, and the targeted DdoS attack will start. This is not the first time that DdoS extortion demands have circulated across the Internet. In 2015, Akamai published research concerning a group calling itself DD4BC (DdoS 4 Bitcoin), which was responsible for a number of DdoS attacks. Apparently clinging to the hope of a major Bitcoin payout, criminal actors have started to ramp up their efforts and their attack bandwidth, which puts to rest any notion that DdoS extortion was old news. Extortion or ransom DdoS (RDDoS) attacks started to become a new threat in 2020 and grew bigger and more complex since then. They started around 200Gbps and then flexed to more than 500Gbps in mid-September. In February 2021, internet security services company Akamai saw its share of a challenge dealing with an 800Gbps RDDoS that targeted a gambling company in Europe. Last September, a threat actor deployed an RDDoS against VoIP.ms voice-over-Internet provider, disrupting phone services as the company’s DNS servers became unreachable.

It is clear that DDoS attacks are not a PSP specific issue, but it is also a threat to the whole financial sector. The threat is well known now in the sector and most PSPs have taken mitigating measures against these kinds of threats (see below).

22 https://www.imperva.com/blog/why-banks-are-still-a-top-target-for-ddos-attacks/

23 https://www.helpnetsecurity.com/2022/03/31/ddos-attacks-becoming-complex/

3.1.4.2 Suggested Controls and Mitigation

PSPs should preferably set up a (DdoS) security control framework. In general terms they should be able to identify, protect, detect, respond, recover, assess and adjust possible DdoS attacks. The table below gives a high-level description of these controls[24].

Level	Description
Identify	Develop the organisational understanding to manage DdoS risk to systems, assets, data and capabilities
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
Detect	Develop and implement the appropriate activities to identify the occurrence of a DdoS attack
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
Recover	Develop and implement the appropriate activities to maintain plans for resilience to restore any capabilities or services that were impaired due to a DdoS event
Assess	Determine whether the previous functions performed/functioned effectively
Adjust	Determine which changes need to be made, based on the assessment made

Table 5 High-level dynamic DdoS security control framework

The Internet Engineering Task Force (IETF) established a new working group called DdoS Open Threat Signalling (DOTS). The aim of DOTS is to develop a standard based approach for the real time signalling of DdoS related telemetry and threat handling requests and data between elements concerned with DdoS attack detection, classification, trace-back, and mitigation.

In general, PSPs are expected to have implemented a so-called "*DdoS mitigation scrubbing service*". This is a service to filter the fraudulent traffic of the DdoS attacks. Scrubbing is more specifically a good mitigating measure against flooding attacks and sometimes mitigating protocol-attacks. Scrubbing services are provided by third party service providers.

Since protocol- and application attacks comply with the standard for the protocol in question, it is more difficult to counteract such attacks. PSPs have implemented or should implement mitigating measures against application level attacks including for instance application-level security products, application level key completion indicators, filtering capabilities, etc.

PSPs can simulate attacks on their environment in order to prove that mitigating measures (including organisation and personnel) are adequate. Moreover, every entity should also test periodically their anti DdoS measures (e.g. through DdoS simulations). This testing should cover both the technical and the organisational aspects (e.g. procedures).

One additional set of countermeasures is to organise security intelligence. It is important to know what types of DdoS and what type of actors and motivations are around; it helps to take accurate measures and to determine the (residual) risk of the organisation of getting hit by DdoS-attacks.

[24] more details may be found in Chapter 5 in http://www.vurore.nl/images/vurore/downloads/scripties/2040-Def.scriptie_LarsDrost.pdf

Security intelligence can be received from a commercial organisation and/or a governmental or industry specific Computer Emergency Response Team (CERT), which are a good answer to deter the effects of DDoS activities.

PSPs should consult their upstream (telecom) provider and the local Law Enforcement Agency to check whether the logging capabilities of the PSP and the monitoring solutions of the PSP offer sufficient capabilities for the PSP to be *"forensic ready"* for law enforcement.

3.1.5 Botnets

A *botnet* is a collection of internet-connected devices compromised by an attacker who orchestrates through a C&C, without the knowledge of the victim.

Botnets act as a force multiplier for malicious activity. Commonly used for DdoS attacks, attackers also make use of the botnets' collective power to scale attacks such as spamming, credential compromise, delivering malware or cryptocurrency mining. The word "botnet" is a combination of the words "robot" and "network". Nowadays, botnets seem to focus more and more on ransomware and not on fraud related activities. Notorious banking malware botnets such as Emotet are an example. Emotet has been one of the most professional and long lasting cybercrime services out there. First discovered as a banking Trojan in 2014, the malware evolved into the go-to solution for cybercriminals over the years. The EMOTET infrastructure essentially acted as a primary door opener for computer systems on a global scale. Once this unauthorised access was established, these were sold to other top-level criminal groups to deploy further illicit activities such data theft and extortion through ransomware. However, the Emotet botnet was 34ddresses34ly taken down in January 2021 Europol announced in a Press Release[1] that Emotet had been disrupted and investigators had taken control of its infrastructure. Thereforethus more than 500 servers from different tiers were taken down of the criminal infrastructure. A database containing e-mail 34ddresses, usernames and passwords stolen by Emotet was compiled by analysing all the seized infrastructure. This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust. This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). And just very recently, in August 2023, a U.S. government operation has dismantled the infrastructure of the notorious Qakbot malware, which officials say caused "hundreds of millions" of dollars of damage worldwide. More than 700,000 infected computers worldwide were identified. The FBI also announced the seizure of 52 servers, Ih it said would "permanently dismantle" the botnet.
The Department of Justice also announced the seizure of more than $8.6 million in cryptocurrency from the Qakbot cybercriminal organization, which will now be made available to victims. The operation, which was carried out in partnership with law enforcement agencies in France, Germany, the Netherlands, Romania, Latvia and the United Kingdom, is described as the largest U.S.-led financial and technical disruption of a botnet infrastructure leveraged by cybercriminals to commit ransomware, financial fraud and other cyber-enabled criminal activity. Qakbot, also known as "Qbot" and "QuakBot," was first detected in 2008, making it one of the longest-running botnets. The malware, which first emerged as a banking trojan, infects devices primarily through phishing emails containing malicious links or attachments. Once a target taps the link or downloads the attachment, Qakbot would deploy additional malware to their computer to become part of a botnet

[1] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

network that could be controlled remotely. In recent years, Qakbot become the botnet of choice for some of the most infamous ransomware gangs, including Conti, ProLock, Egregor, Revil, MegaCortex and Black Basta.Botnets have two main objectives:

- Herding more devices into the botnet and;
- Performing malicious activity.

The malicious activity performed by a botnet can be of a wide variety, namely:

Distributed Denial of Service (DdoS)

Botnets usually consist of such large numbers of remote machines that their cumulative bandwidth can reach hundreds of gigabytes of upstream traffic per second. This enables botmasters to start targeted sabotage attacks against websites. The usage of botnets that are becoming more and more intelligent will create flexible tools for the execution of DdoS attacks.

Spam email

One of the most popular uses of botnets was spamming. The ability of botnets to use bots' IP addresses to hide the true originator of the spam email complicates countermeasures such as the blacklisting of suspicious IP addresses. Nowadays phishing is done less by botnets as more SIM cards are being used ("smishing") for this purpose.

Credential harvesting

A major use of botnets, with the intention of gaining financial benefits, is for the automated extraction of user data and credentials from infected hosts.

Man-in-the browser malware to intercept online banking credentials is one of the attack vectors that can achieve a large-scale attack through the use of a botnet.

Account testing fraud

Cybercriminals can scan a range of IP addresses to find a specific port, and then bombard the service – FTP, Telnet, RDP or others – with rapid-fire authentication credentials from a list they have developed or bought in the underground market.

In the electronic payments sector this can be used to test credit card numbers or online banking accounts.

Cryptocurrency mining

Cryptocurrency mining requires intensive computing power. Botnets are a preferred means to mine crypto-currency drawing on the victim's system computing power and electricity.

Many other malicious activities may be performed benefitting from the large scale offered by botnets, such as:

- Click and pay-per-install fraud;
- Manipulation of online polls;
- Denial of inventory;
- CAPCHA solving;
- Hosting illegal downloads.

3.1.5.1 Impact and Consequences

A few evolutions have occurred to botnets in the last years, in respect to their C&C strategy, to the types of infected devices, to the malicious activity and to the commercial model of botnets.

C&C strategy – Centralised to decentralised

The most important part of a botnet is the so-called C&C infrastructure from where the attacker can control the botnet giving instructions to the bots and receiving collected data from them.

The first botnets would have a centralised approach comparable to the classic client-server network model.

Newer botnets use a decentralised, i.e. peer-to-peer, model in order to try and evade detection and to be more resilient in face of takedown attempts.

The bots maintain connectivity to other bots and issue requests for new commands to the botnet. Because there is no single set of command servers that can serve as a single point of failure, and the botmaster can hide inside the network of bots when giving commands, this approach is harder to mitigate.

Types of infected devices – Computers to IoT

The compromised systems in traditional botnets were almost exclusively computers, recent botnets compromise IoT devices such as cameras, routers, Digital Video Recorders (DVRs), wearables and other embedded technologies. IoT botnets tend to be larger in scale due to a set of characteristics of the compromised systems:

- IoT devices are usually designed with lowering costs as a major driver and security interests tend to be neglected. As a result, these embedded devices are easily exploited (e.g., default credentials, exposed services).
- These devices are in many cases not subject to patching or firmware upgrades leaving large numbers of devices subject to exploitation of already published vulnerabilities.
- Many of these devices are permanently online and available 24x365, resulting in a larger exposure surface from the beginning of an exploit.
- Devices are rarely monitored, preventing timely detection.

Botnet malicious activity – Crypto-currency mining

Botnets are the basis for certain types of attacks such as DdoS and spam mailing; and are a way to enlarge the scale of other attack types.

One use of botnets that fits perfectly the objective of the attackers is by using the bots for crypto-currency mining. The vast computing capacity managed through the botnet's compromised devices and the tremendous usage of electricity power, both supported unknowingly by the victims, are beneficial for financial gains through crypto-currency mining. The fact that no apparent harm is sensed by the victim makes detection less probable and turns the botnet even more profitable.

Commercial model of botnets – Botnet kits

For some years, botnets have been offered as a commodity either through selling subparts of the botnet or by leasing botnets. More recently botnet kits have been behind some major botnets. .

3.1.5.2 Suggested Controls and Mitigation

The CSDE (Council to Secure the Digital Economy) has published the "International botnet and IoT security guide – 2021"[25] that highlights practices to combat botnet threats. This report details a wide range of mechanisms and processes that mitigate the effects of attacks conducted through

[25] https://csde.org/wp-content/uploads/2021/03/CSDE-2021-Botnet-Report-March-24-2021.pdf

botnets. It divides the measures applicable to "Infrastructure", "Software development" and "IoT Devices" and further details measures for "Home and small business systems installation" and for "Enterprises".

Authorities should agree with ISPs on limiting Internet access to customers who are (suspected of being) part of a botnet and isolating these customers in a quarantine network and integrate these agreements in SLA's with these ISPs.

The ENISA report "Botnets: Detection, Measurement, Disinfection and Defense"[26] continues to be a reference for mitigation techniques for botnet threats, covering both technical methods and social and regulatory approaches.

Technical countermeasures

- Blacklisting
- Sinkholing
- Orchestration of controls at host and network level
- Vulnerability management in combination with regular updates
- Distribution of fake/traceable credentials
- DNS-based countermeasures
- Direct takedown of C&C server
- Packet filtering on network and application level
- Walled gardens
- Peer-to-peer countermeasures
- Quarantine Infected Computers
- Infiltration and remote disinfection.

Regulatory and social countermeasures

- Dedicated laws on cybercrime
- User awareness raising and special training
- Central incident help desk
- Enhance cooperation between stakeholders.

3.1.6 Third-party compromise, supply chain attacks and outages

It is quite common that banks, and in general PSPs, rely on third-party vendors to provide services and products to their customers. For example, processes outsourced by banks may include customer service, credit cards, data entry operations, ATM services or even entire business functions such as risk management and IT support.

It is clear that third party vendors are critical for every organization's business, especially for PSPs – but they also introduce cyber risk. In fact, targeting the trust relationships, insecure PSPs' suppliers in the chain can become the point of access to their larger partners. This kind of attacks are known under the name of **supply chain attacks**.

[26] https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

According to ENISA[27], a supply chain attack is a combination of at least two attacks. The first attack is on a supplier that is then used to attack the target to gain access to its assets. The target can be the final customer or another supplier. Therefore, to classify an attack as a "supply chain attack", both the supplier and the customer have to be targets.

A distinction can be made between two basic types of supply chain attacks:

- **In software supply chain attacks** –malicious actors exploit the software vendor of their targets. It is accomplished by compromising staged of the software development lifecycle. Most of the times, attackers target software updates. Threat actors first gain access to the software's update server and then inject malicious code into the update packages. Once that the target organization download and install the malicious packages from its suppliers, malicious actors can gain access to the organization's network.
- **In hardware supply chain attacks** physical components are tampered with. For example, a manufacturer can install a malicious microchip on a circuit board used to build servers and other network components. These kind of supply attacks are very rare as they require the cooperation of manufacturers and vendors.

Although not always present in the literature, it is worth to mention also the risks introduced by the use of open-source software libraries as they are widely used due to decrease development time and costs. Should a third-party library developer inject malicious code into the product, any software developer that incorporates the infected library would be vulnerable.

Despite the fact that supply chain attacks have been a security concern for many years, they increased in number and sophistication. Among the most important and recent incidents it is worth to mention Solarwinds, Accellion, Kaseya, and Log4j that affected many organizations from all over the world.

In the light of a such strong interconnectivity among systems and processes across network and organizations, PSPs need to manage such risks in order to prevent data breaches, financial losses, and operational failures.

3.1.6.1 Impact and Consequences

Unfortunately, due to the lack of visibility on third-party vendors, supply chain attacks are hard to detect for any organization.

Successful supply chain attacks can lead to catastrophic consequences. Once a threat actor bypasses the security perimeter of the target through software vendor, it can maintain persistent access for a long time. In addition, if the threat actor loses the access to the victim's network, he can re-gain access through the compromised software vendor.

Such kind of attacks have severe impacts which can devastate corporate revenue, brand reputation, and vendor relationships.

The main impacts from supply chain attacks are listed below:

- **Data breaches and data disclosure**: Any data that passes through a system infected with the malicious code could be breached, including potentially stealing high-privileged

[27] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

account credentials for future compromises, corporate information and financial information.
- **Malware installation**: Ransomware, rootkits, keyloggers, viruses, and other malware could be installed using injected supply chain attack code.
- **Reputational damage**: loss of customers, loss of sales, reduction in profit can be some of the negative effects caused by supply chain attacks.

But, fortunately, no incident has yet significantly impaired PSPs. Anyway, it is worth to provide some examples to illustrate how a cyber incident may have impact on PSPs and the financial system.

Among the most sophisticated and disruptive attacks seen in the past, we highlight the incident happened in 2020 that affected SolarWinds and its customers. SolarWinds customers, which included large financial institutions, were infected by the malware when they installed the software update. The attack opened a backdoor through which attackers could have exploited the customers' computer systems. As previously mentioned, no PSPs appeared to have been the intended targets of such attacks. However, if they had been, the consequences for the interested PSPs and the whole financial sector could have been devastating.

Worth to mention are also the risks associated to digital operations when providers experience long outages. For example, in 2019, Google experienced a network outage that impacted services hosted in some of the US regions of Google Cloud Platform. The outage lasted for more than four hours and affected access to various services. In that case, if PSPs had transitioned their business activities to the cloud, the outage could have disrupted bank's payments services. Another example is that of a major bank that in 2016, due to an outage cause by a technological issue inside one of the platforms hosted by the bank itself, was unable to process payment instructions sent over the SWIFT network from clients for 19 hours[28]. Finally, we report the case of an outage of a bank's data centre caused by a smoke condition[29]. It caused an automatic shutoff of power to the centre resulting in the unavailability of some customer accounts through online/mobile banking applications and ATMs.

The previous examples show in what measure the PSPs physical and digital operations are heavily interconnected, and problems in either can affect the other.

3.1.6.2 Suggested Controls and Mitigation

The management of relations with suppliers – and consequently with any sub-suppliers – is of crucial importance in banking and financial legislation. Until now, however, this importance was reserved only for IT service providers to whom financial entities outsource essential or important services or functions, providing for mostly general rules. Furthermore, the regulation of relations with these service providers was given by monitoring and control obligations incumbent solely on banks and financial institutions, which therefore included these obligations in the contracts with their ICT service providers, without however there being a clear system of rules which specifically

[28] https://www.pymnts.com/bank-regulation/2016/bny-mellon-unable-to-run-payments-for-19-hours/

[29] https://www.cnbc.com/2019/02/08/wells-fargo-says-working-to-fully-restore-system-as-outage-spills-into-day-2.html

and clearly and targetedly regulated the content of the contractual provisions stipulated with these subjects.

This meant, as an immediate consequence, that the effectiveness of the contractual clauses – including those on IT security measures – depended on the success of the construction and, to a large extent, on the contractual power of the service provider.

The DORA [6] Regulation starts precisely from these premises, establishing, in Chapter V, the fundamental principles that must guide the management, by financial entities, of IT risks deriving from third parties, which are considered as an integral part of their own risks.

To this end, it should be noted that DORA does not only deal with outsourcers of ICT services, but speaks in general of "ICT service providers", which means that the spectrum of subjects with whom financial institutions must adequately regulate their relationships is broadened, extending it to all types of ICT service provision (for example, the supplier of hardware devices that carries out maintenance and assistance on them will also be the recipient of the legislation). The following points provide some provisions aimed to strengthen the digital resilience financial operators involving third-parties services providers:

- In order to understand the complex interconnection and any vulnerabilities, DORA will require the mapping of all ICT systems and assets of financial institutions. Third-party services providers are included in such mapping.
- DORA will enable regulators and financial institutions to perform audits throughout the supply chain in the financial industry.
- DORA will require the definition of a third-party management framework such as the nomination of executives responsible for operational resilience.
- DORA will require firms to set specific requirements for outsourcing ICT systems and services to third parties. In addition, critical third-party providers are obliged to comply with the same rules as financial institutions.

Therefore, should be highlighted that as best practice, each PSPs should apply a risks assessment process able to identify dependencies on third-party suppliers of these services and assets. Such analysis should identify critical IT supplier dependencies, customer dependencies, the mapping of critical software and single point of failure[30].

To conclude, it is worth to mention also the eight key practices suggested by NIST for establishing a Cyber Supply Chain Risk Management (C-SCRM) approach that can be applied to software[31]:

1. Integrate C-SCRM across the organization.
2. Establish a formal C-SCRM program.
3. Know and manage critical components and suppliers.
4. Understand the organization's supply chain.
5. Closely collaborate with key suppliers.
6. Include key suppliers in resilience and improvement activities.
7. Assess and monitor throughout the supplier relationship.
8. Plan for the full lifecycle.

[30] https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

[31] Jon Boyens, et al., "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry", NISTIR 8276
(February 2021), https://doi.org/10.6028/NIST.IR.8276

These practices can assist PSPs in preventing, mitigating, and responding to software vulnerabilities that may be introduced through the cyber supply chain and exploited by malicious actors.

3.1.7 Monetisation Channels

A fraudster, who has succeeded to establish a fraudulent payment transaction (whether authorised or unauthorised), knows of course that investigators soon will follow the trace and that the transaction amount may be frozen or returned. He therefore aims at immediately leveraging a monetisation channel: a cash withdrawal, a purchase (that leaves no trace), a money transfer or a transfer to another bank account from which again a withdrawal, purchase or transfer may be initiated. Purchases that leave no trace may include buying crypto currencies or acquiring gambling credits or goods that can easily be cashed in over the internet. Common examples of such goods include airline tickets and any type of vouchers or gift cards but may also include more expensive items such as jewellery or electronic equipment.

However, especially in a corporate context the fraudster's monetisation options are not limited only to the immediate use of liquid funds available via the victim's payment account, credit card, etc. but may include also cover acts such as brokering access to breached systems, data or user accounts, modification or encryption of data for subsequent extortion purposes, etc.

3.1.7.1 Impact and Consequences

To stay in the shadows the fraudster hires 'money mules' and uses their bank accounts to receive the fraudulent transfers and the mules themselves – according to the fraudster's instructions – to bring the spoils to the fraudster in a way it cannot be tracked. The mule is either willingly or unwillingly, knowingly or unknowingly covering the tracks of the fraudster. The emergence and rapid expansion of crime-as-a-service has made money muling services readily available via darknet marketplaces and instead of recruiting them the fraudster can choose to hire money mules as and when needed.

Most mules will eventually be subject to investigations and reported to the police. If there are any funds left on a mule's account after paying the fraudster, the mule will likely be forced to return the amount that was stolen from the original victim. Hence, it seems that a mule is bound to lose, but nevertheless new recruits are constantly being persuaded to act as such[32].

When a fraudster has established the necessary mule(s), the fraudster will orchestrate the combination of conducting one or more fraudulent transactions and using the mule(s) to get the money out of sight. The actual flow may depend on the size of the amount(s) and the needed level of complexity to escape investigators. Especially cross-border transfers and more in particular instant payments make investigations and fund recovery more difficult and complex.

Two examples of possible flows involving money mules are provided below. While complexity makes it harder for investigators, it also increases quite dramatically the fraudsters' effort and risks. Most cases therefore are not very complex and do not involve more than one or two levels of mules, although when needed professional mules can be sourced "as a service" to make things easier for a fraudster.

[32] See a comprehensive description of "The money mule trap" at FINTRAIL

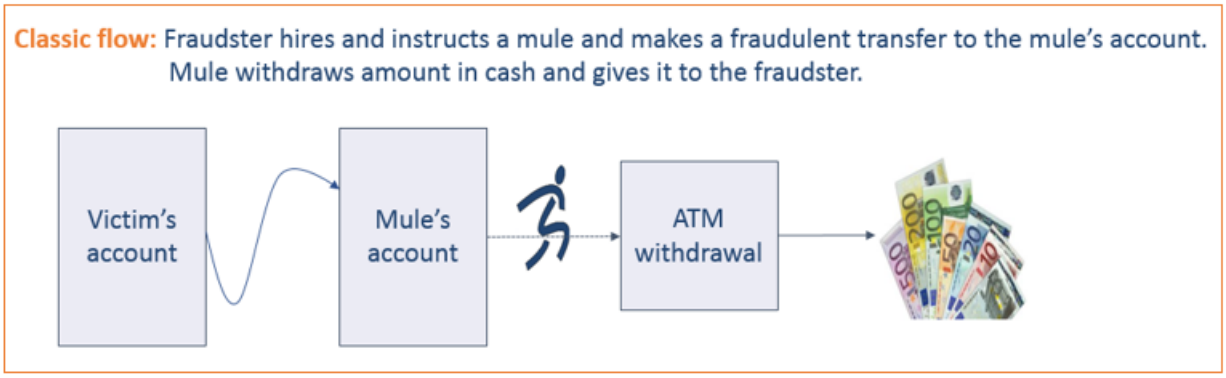

Figure 1: Classic money mule flow

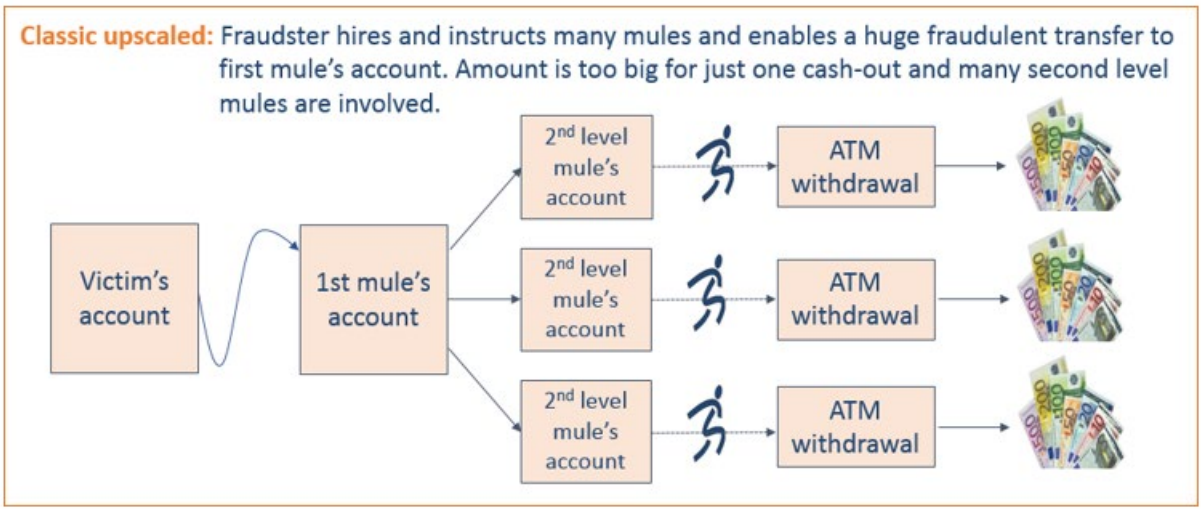

Figure 2: Classic upscaled money mule flow

A critical step is when the money finally leaves the banking system through any kind of transaction that covers the tracks sufficiently for the criminals. In the flows above the mule withdraws cash and often sends it to the fraudster via money transfer service to preserve anonymity. However other modi operandi may be employed in which money mules can be avoided or digitised:

- By directly purchasing valuable assets (ideally digital) which can easily be cashed-in over the internet;
- By directly initiating a fraudulent payment to a money transfer service account (such service supporting withdrawal around the globe with varying levels of identity verification);
- By directly buying hard-to-investigate or hard-to-trace crypto currencies.

Anonymity of crypto currencies exploited as a replacement for mules

While money transfer services have always played a key role in enabling fraudsters to hide behind the money mules, anonymous virtual currencies have been identified as an often much more efficient replacement for both. Virtual currencies are defined by the European Banking Authority (EBA) as "a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat currency but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically"[33].

[33] https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

Over the last few years, popularity of virtual currencies has skyrocketed, due to the surge of decentralised digital currencies, like Bitcoin, the first to appear in 2009 and still the most important of them. Decentralisation means that one person can pay directly to another without using a third party as an intermediary, something that before was only possible using cash. It is for this reason that decentralised digital currencies are commonly considered "digital cash" and currently achieve a market capitalisation of more than 200 billion euros[35].

In Bitcoin-like schemes, trust is provided by a mix of technologies that include primarily cryptography, instead of being provided by a trusted third party. Therefore, these kinds of decentralised currencies are also referred to as cryptocurrencies. As such they allow for reliable, fast and irreversible online transactions, are not centrally controlled, have no built-in know-your-customer (KYC) mechanism, and are relatively difficult to trace. Therefore, they have also become a magnet for criminals. Indeed, their illicit use is increasingly happening as criminals are gradually accepting it as a currency of choice for trade in the darknet.

Although all crypto currency transactions are stored publicly and permanently on the network by means of blockchain technology, the identity of a user behind an address can remain unknown. Moreover, *Bitcoin mixer* services have appeared, with the aim to provide obfuscation of the flow of funds in exchange for a fee, allowing fraudsters to move and cash-out the stolen funds anonymously.

3.1.7.2 Suggested Controls and Mitigation

Money mules, anonymous or non-traceable money transfers, crypto currency services, but also instant payments make it easier for fraudsters and harder for fraud investigators.

Raise Awareness

It is not generally understood that when a person receives some money (e.g. via a mobile P2P or banking app) – withdraws the same amount from an ATM and passes on the cash to some friendly person they just met, they might have in reality helped to cover up a crime. Awareness is especially necessary towards youngsters, who due to natural lack of experience, low income, willingness to-help-out and sometimes some "peer pressure", seem more prone to become mules. PSPs should be careful to give easy-to-understand warnings against "becoming a mule" when they provide access to on-line banking services or issue payment cards. Awareness must also target other identified "vulnerable" groups (such as low-income persons, addicts, etc.) tempted by seemingly easy money and unaware of law and consequences[36].

Register/ share identified mules

For those mules, who know what they are doing and do it for the gains they can achieve, awareness is not relevant. Instead, PSPs should cooperate to achieve that the same person cannot act as colluding mule again and again by shifting to a new PSP. It should be possible to register in a common database if a person repeatedly has acted as a mule, subject to respect of data protection laws (e.g., GDPR). This should not necessarily hinder this person to open a payment account, but it should enable monitoring to detect possible new mule activity by this person at a very early stage.

Monitor, detect and stop mule-like behaviour at PSP and regulator level

[35] Cryptocurrency market capitalisation is available at https://coinmarketcap.com/

[36] See "The money mule trap" at FINTRAIL

Regulators and PSPs should consider having mechanisms in place to react and stop supporting service practices or to put related transactions on hold, until further investigated, if transaction patterns indicate ”mule activity”” – e.g., if larger amounts arrive from or flow to new (unknown) sources, followed by attempts to cash out or pass on these amounts via other ways.

Detect complex mule and money laundering schemes

For a single PSP it may end up being very difficult to “follow the track” if there are many mule-levels and cross-border payments are involved. However, if PSPs cooperate[37] and pool their payment data (in a secure and lawful way), it may be possible to use strong analysis tools and much more efficiently detect mule accounts and money laundering rings. Whereas the first mule level has a short lifetime, subsequent mule-levels may re-use accounts over a longer period if they can stay undetected. Analysis on pooled data can put a significant pressure on money mule schemes[38]. To be effective in the long run such cooperation must be cross-border and will become even more important in view of instant payments, which are expected to gradually become the new normal.

3.1.8 Liability for Social Engineering Fraud

Social engineering (c.f. Section3.1.1) aims at tricking the customer in a self-exposing behaviour he or she is not supposed to adopt. As a consequence the customer at first hand appears liable for his or her own misbehaving. The fact that APP fraud or fraud more generally related to scams has been rapidly growing over the last years has raised attention among regulators on how to possibly counter this evolution with liability shifts.

Discussions started in the UK, where the Payment Systems Regulator mandates sending and receiving PSP, as of 2024, to reimburse in most cases customers that fall victim of APP fraud[39]. Also in Asia the MAS announced back in 2022 that their Payment Council is working on a framework for equitable sharing of losses arising from scams[40], not yet released.

In the EU, the recently proposed regulation for payment services (PSR) addresses the topic as well[41]. The proposal grants customer refund rights in two situations: for consumers who suffered damages caused by the failure of the IBAN/name verification service to detect a mismatch between the name and IBAN of the payee, and for consumers falling victim of a spoofing fraud where the fraudster contacts the consumer pretending to be an employee of the consumer’s bank, tricking the consumer into carrying out some actions causing financial damages to the consumer.

Discussions are still ongoing also at national level and are neither conclusive nor fully aligned on the topic. Nonetheless, there is an observable tendency to increase PSP’s liability for not detecting fraud occurring because of social-engineered customer misbehaviour.

---

[37] See New anti-money laundering technology sees UK fraud rings frozen

[38] https://www.europol.europa.eu/newsroom/news/over-1500-money-mules-identified-in-worldwide-money-laundering-sting

[39] See https://www.psr.org.uk/publications/policy-statements/ps23-3-fighting-authorised-push-payment-fraud-a-new-reimbursement-requirement/

[40] See https://www.mas.gov.sg/news/media-releases/2022/a-framework-for-equitable-sharing-of-losses-arising-from-scams

41 See https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543

3.2 Fraud per Payment-Relevant Process

3.2.1 Introduction

This section describes various attacks that may lead to fraud, occurring in all payment-relevant processes of a business transaction. Often attacks are caused by exploiting a combination of several threats. Multi-vector attacks are becoming commonplace and have been targeting a number of financial institutions (e.g. recent examples of multi-vector attacks include cyberattacks using the SWIFT-related banking infrastructure, ATM infections, remote banking systems and POS terminal networks[42], making changes in PSP' databases to "play" with account balances, as well as supply-chain attacks, i.e. attacks on vendors supplying financial organisations[43]).

The table below provides a non-exhaustive view on possible impact of threats and fraud enablers on payment-relevant processes.

	Social engineering	Malware	APT	DoS
On-boarding/ Provisioning	X	X		
Request-to-Pay/ Invoicing	X	X		
Initiation/ Authentication	X	X		
Execution	X	X	X	X

3.2.2 On-boarding and Provisioning

There are essentially four types of attacks against on-boarding or provisioning processes:

- Manipulate client information in an authoritative registry e.g., change the surface mailing address for hardware credentials (authenticator or payment cards) or the mobile number for SMS one time passwords (OTP) and then trigger a delivery to the modified destination.
- Exploit oversimplified ordering of new or replacement credentials to a registered address, with the intention to physically steal the credentials from the client's mailbox upon delivery by the post services.
- Fake enrolment with stolen onboarding or login credentials to a payment app, mobile bank app or general authenticator app. If login credentials can also be used for activation this is very convenient, as it allows the fraudster to delay payment execution until any time later that better suits the attack.
- Request Subscriber Identification Module (SIM) Swapping or Duplication from the mobile network operator in case the bank uses SMS OTP and the network operator's client authentication procedure is easier to overcome than any of the bank's procedures.

Manipulation of identity-relevant information

Already in the on-boarding process a fraudster could be involved. The purpose for the fraudster can be e.g., to obtain tax returns intended for the victim, take out loans in victim's name, establish a mule account, get a credit card with a spendable limit and others. KYC and AML laws and

[42] See for example: https://www.tripwire.com/state-of-security/security-data-protection/hackers-indian-bank-attack/

[43] https://securelist.com/cybercriminals-vs-financial-institutions/83370/

regulations oblige banks and other account servicing institutions to apply a thorough scrutiny, when opening new customer relationships.

'Verifying the identity of a new account holder' and 'providing a new account holder with an authenticator for payments may seem two independent procedures, but the quality of the first largely impacts the second. There is a certain point in the 'onboarding dialogue' – whether face-to-face or online – where the new account holder is identified and where sensitive information is securely exchanged. During onboarding, every information that is relevant for a secure provisioning of authenticators or for later secure authentication, e.g. with Q&A over the phone, must be collected in a reliable way. This may include:

- home address (verified by authoritative registry),
- telephone number
- email address,
- copy of passport, driver license or other types of ID documents
- Activation code for an authenticator
- Control questions with a set of answers only account holder should know
- biometrics (e.g. pictures, fingerprints or other)

Exploitation of oversimplified ordering of credentials

Often triggering a surface mailing to a preregistered address is deem insensitive and can be initiate without any strong authentication. However, If the client is known not to be at home during delivery or has a mailbox that is easily accessible for a fraudster, the fraudster may exploit the oversimplification of the ordering / reordering process to get physical hold of a spare set of credentials.

Fake enrolment with stolen credentials

Whereas a secure and correctly enrolled mobile authentication/payment app may be hard to attack, the enrolment procedure itself may be weaker and therefore become a preferred target for fraudsters. The enrolment may require information that can easily be phished or vished or guessed, may depend upon approvals by the victim easily persuadable through some sort of scam or may simply be exposed to manipulation by malware in every authenticated online banking session (e.g. registered a mobile number). If so, the fraudster may be able to perform a fake enrolment to a mobile authenticator that can be misused afterwards to authorise any payment at any point in time.

SIM swapping or duplicate SIM attacks

SIM swapping or duplicate SIM ordering are legitimate services offered by mobile network operators. The reasons for carrying out the swap are to enable the user to move to other mobile network operator, to disable and replace a SIM card following a lost or stolen mobile device, to change the SIM card for a new one of a different form factor or to get a duplicate card to permanently install on another device or in a car.

SIM swap fraud happens when fraudsters transfer a customer's mobile number to a fraudster's SIM. Duplicate SIM fraud happens when fraudsters order a duplicate SIM to a modified address or collect a duplicated SIM in a provider shop. Fraudsters leverage such attacks to acquire security messages with one-time passwords (OTP) sent to the customer by the PSP, for reconfirmation of sensitive operations such as specific payments (e.g. 3D Secure for online card transactions), changes to the customer profiles, whitelisting of beneficiaries, provisioning of card tokens to wallets and then leverage those to perform fraud.

3.2.2.1 Suggested Controls and Mitigation

The general advice is that the security level for the enrolment or ordering of credentials (authenticators or payment cards, must be as strong as (or preferably: stronger than) the authentication and confirmation of a high-risk payment. This means that the enrolment should rely on 'factors' that cannot be compromised by the same method. In addition, it may be considered to send notifications and, in case of authenticators, to only allow the authenticator to give access to information (not payments) for a quarantine period of 1 or 2 days.

Biometrics capture during online on-boarding may also offer an interesting alternative to be used as a possible authentication 'factor' during authenticator app enrolment. Face, voice, fingerprints, veins in the hand or in the eye are characteristic features that can allow for a strong and otherwise independent authentication in such a situation. The smart phone, moreover, can supports the app in capturing these biometrics. But three key questions nevertheless arise:

- What can these biometrics be compared with for authentication, i.e., does the issuer of an authenticator app have access to reference data from the on-boarding process?
- Does the technology perform as needed and expected, i.e., is it user-friendly and are true users accepted and imposters rejected both with high probability?
- Is it cost-efficient and can it be smoothly integrated with the 'identity verification' process in place or established to cover for KYC and AML during on-boarding?

As of now there is no clear answer yet to these questions and most of this data will likely become available only with the spreading of modern selfie or video based online on-boarding processes. Nevertheless, it is deemed worth early exploring these possibilities as a valuable means against false enrolment of authenticator apps.

SIM swap and SIM duplication fraud detection identifies suspicious SIM usage patterns. It ranks the risk based on location, device type and customer behaviour. Different risk levels trigger different corrective actions, such as blocking transactions, locking accounts, or sending customer communications. There are a number of controls that end users can implement to try and prevent, or at least quickly detect, SIM swapping:

- Enquire with your mobile operator if you have no network connectivity and you are not receiving any calls or SMS for unusually long periods;
- Keep personal details that would be useful to a fraudster, i.e. phone number, date of birth etc. off social media sites;
- Ask your mobile payment service provider to give you details of every financial transaction through two channels – for instance, SMS as well as email alerts.

In addition, a mobile payment service provider can negotiate with the mobile operators that they are informed about the SIM swaps or duplicate SIM issuing. This can help in monitoring the usage of the account.

During the last years there has been a considerable increase in the use of the mobile device, whether via SMS, call or mobile application as the authentication mechanism. Technological solutions to try and secure the mobile device and enable out-of-band authentication via the device continue to be developed and implemented. If credentials have been phished successfully and the attacker tries to abuse them to make a fraudulent transaction, there may still be hurdles to overcome (c.f. Section 3.4).

3.2.3 Request-to-Pay and Invoicing

Although the invoicing (paper-based or e-invoicing) and Request-to-Pay[44] (RTP) are processes that, in an end-to-end business transaction, are outside of the payment chain, they are particularly exposed to fraud as they rely on the trust between the Payee and Payer and the security of the environment in which this information is exchanged. Therefore, they give rise to a specific vector of fraud for subsequent payment processes.

Often, fraud on invoices or RTP messages leads to Authorised Push Payment (APP) fraud at the payment stage, as the payers initiate related payments in good faith, by accepting the terms presented in the invoice or the RTP. Moreover, when received through trusted channels such as an e-banking interface, the RTPs or e-invoices are treated as verified and their senders trusted by the Payer's PSP. Another reason that e-invoices/RTP are often trusted is that they appear to be sent by government departments (for taxes, fines), the police, healthcare institutions or from utilities or telecommunication operators. If by extension, any claim for payment is considered a form of RTP, the invoicing and RTP fraud patterns can give rise to a fraud category commonly referred to as APP fraud.

Authorised Push Payment (APP) fraud, in which the victims – being subject to a scam – actually make the payment themselves, is showing a steep increase and for PSPs is much harder to detect. At the root of any APP scam is a "convincing" lie with which the fraudster somehow manages to deceive the victim.

In the "Fraud-the-Facts 2023" report[45] from UK Finance, the following types of APP scams can be found:

- *Purchase scam*: the victim pays in advance for goods or services that are never received. These scams usually involve the victim using an online platform such as an auction website or social media.
- *Investment scam*: a criminal convinces the victims to move their money to a fictitious fund or to pay for a fake investment. The criminal will usually promise a high return in order to entice victims into making the transfer. These scams include investments in items such as gold, property, carbon credits, cryptocurrencies, land banks and wine.
- *Romance scam*: the victim is convinced to make a payment to a person they have met online through social media or dating websites, and with whom they believe they are in a relationship.
- *Advance fee scam*: a criminal convinces their victim to pay a fee which they claim would result in the release of a much larger payment or high-value goods. These scams include claims from the criminals that the victim has won an overseas lottery, that gold or jewellery is being held at customs or that an inheritance is due. The fraudster tells the victims that a fee must be paid to release the funds or goods, however, when the payment is made, the promised goods or money never materialise. These scams often begin with an email or a letter sent by the criminal to the victim.
- *Invoice or mandate scam*: the victim attempts to pay an invoice to a legitimate payee, but the criminal intervenes to convince the victim to redirect the payment to an account they control. It includes criminals targeting consumers posing as conveyancing solicitors, builders and other tradespeople, or targeting businesses posing as a supplier, and claiming

[44] https://www.europeanpaymentscouncil.eu/document-library/rulebooks/srtp-scheme-rulebook-version-21

[45] https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf

that the bank account details have changed. This type of fraud often involves the criminal either intercepting emails or compromising an email account.

- *CEO fraud*: is where the criminal manages to impersonate the CEO of the victim's organisation to convince the victim to make an urgent payment to the scammer's account. This type of fraud mostly affects businesses.
- *Impersonation of police / PSP staff*: in this scam, the criminals contact the victim purporting to be from either the police or the victim's PSP and convinces the victim to make a payment to an account they control.
- *Other impersonations*: a criminal claims to represent an organisation such as a utility company, communications service provider or government department. Common scams include claims that the victim must settle a fictitious fine, pay overdue tax or return an erroneous refund. Sometimes the criminal requests remote access to the victim's computer as part of the scam, claiming that they need to help "fix" a problem.

These scams may be perpetrated using only persuasion, but the fraudster sometimes may include other elements from the fraudster toolbox like vishing and abuse of credentials or malware on the victim's device.

- Specific fraud patterns targeting invoicing/e-invoicing processes:
- As mentioned above, in the 2023 fraud report of UK Finance, an invoice scam could take form of an illegitimate information to payers that the account number (IBAN) of a legitimate payee has changed. This can be called IBAN-fraud or IBAN manipulation whereby a fraudster intercepts and manipulates a paper invoice or an invoice in digital format (e.g. unstructured PDF invoice, or structured e-invoice in a standardised format).

Regarding paper-based invoices for example fraudsters intercept these by taking them out of the mailboxes of the payers and only change the respective IBAN of the payee. This might also be the case for attached paper-slips. Because of the fact that all the other information is unaltered the invoice still looks legitimate. Examples are also known where such manipulation took place at the post office before delivery.

In cases QR-codes which contain payment-data are used as part of an invoice, only the information in the QR-code might be altered by fraudsters, in particular the IBAN of the payee. The parts of the invoice which are readable by the payer may show unaltered and therefore correct IBANs related to a specific company.

In another scenario a fraudster produces fake invoices from scratch, using names and logos of common corporates, such as utilities, insurance companies or big brands. These invoices are then sent by mail or manually put in the mailboxes of potential victims.

- A new form of fraud has been detected in late 2020 and 2021 in some countries, involving different instant payment solutions using the mobile phone of the victim. The fraudsters send a request for money while convincing the victim that it is a payment that they are eligible to receive, for example, a refund of Government fees/taxes. Once convinced, the victim accepts the request to pay thinking that he will receive the money and instead of that, the money is taken from his bank account[46].

[46] https://www.elcorreo.com/tecnologia/internet/consiste-estafa-bizum-20210506135720-nt.html

For e-invoices, the same patterns apply although they are commonly distributed via email to a much higher number of potential victims, increasing the possibility for triggering fraudulent payments.

A review of fraud patterns that specifically target RTP processes must consider that:

- RTP is a service still in the early stages of implementation with various levels of maturity and availability in the European market. The e-invoicing cases already mentioned are in some extent applicable also to RTP.
- Fraudsters that have been successfully onboarded to an RTP service might distribute very large amounts of illegitimate RTP messages, counting on a significant number of payers that do not check the underlying business (payee) and simply authorise their PSP to initiate a payment transaction to pay the amount in the respective request. The effectiveness of this fraud vector is further enhanced by RTPs presented within the payer's online banking to make the payment transaction authorisation process simpler and faster.
- It is still too early for a more complete assessment of the specific threats and fraud patterns that impact RTP services. Nevertheless, it is worth mentioning that the v3.0 of the Rulebook of the SEPA-wide RTP Scheme started to apply in November 2023 and that Scheme Participants started being onboarded in Q4 2021.

3.2.3.1 Suggested Controls and Mitigation

Scams aiming to carry out APPs resulting from fraudulent invoicing and RTP processes are very different and require more elaborate warnings. Specific customer segments may be more exposed to some types of scams than others. For instance, corporate customers are more exposed to invoice scams and CEO-fraud and the awareness campaigns must be tailored accordingly. In the private segment elderly/vulnerable customers appear to be targeted. The use of special awareness campaigns that target certain vulnerable groups may be an APP fraud mitigation control that PSPs consider. But since it may be difficult to reach the target groups effectively, it is recommended also to run more general campaigns that include a suggestion to discuss the risks with friends and family members who may be vulnerable. PSPs may further consider introducing payment limits or geo-blocking features as is common with card payments. The restrictions could by default depend on customer profile, but still be configurable for the individual.

Same as with phishing, the service provider's "central monitoring" may find a transaction "suspicious", put it on hold and request customer reconfirmation via a secure out-of-band channel. Whenever a payment service user is prompted to approve or confirm a payment, the transaction data – especially amount and payee – must be clearly displayed on the user's device, supporting the user in better identifying certain APP scams.

Certain countries like the Netherlands or the UK have established dedicated "**Confirmation of Payee**" or IBAN/payee name matching services. When a payer wants to make a payment, he enters on his device (e.g. mobile phone) not just the account number, but also the name of the beneficiary. The payer's PSP than first validates the match between the account number and the beneficiary's name with the beneficiary's PSP or a service acting on behalf of that PSP. If there is no match or only a partial match, the payer is informed and may decide not to proceed with the payment. Certain types of APP fraud – especially invoice fraud – can specifically be countered by such a service. It must be noted that the European Commission proposals for a regulation as

regards instant credit transfers in euro ("instant payments regulation"[47]) and the PSR[48] also include provisions for such a service.

3.2.4 Payment Initiation & Authentication

Payment Initiation & authentication attacks refer to those that focus on the end clients' systems and thus are distinct from the scam-based attacks described in the previous section that tend to target the end clients themselves or the channels through which they get invoices or RTPs.

Payment initiation and authentication is primarily exposed to malware attacks. During the past years we have seen malware evolving from key logging, capturing of online banking credentials or credit card numbers, to man-in-the browsers taking advantage of virtual keyboards RATs and memory scraping functionality. The most important and persistent banking malware is Emotet which is described in chapter 2.5. Many other strains of specialised malware have surged targeting banking credentials, targeting credit card numbers, targeting POS systems with the intention to gather PINs and card data, or targeting ATMs with the intention to enable jackpotting attacks.

Such malware may either directly manipulate transactions or steal credentials entered by the customers towards misusing them at a later stage. It is common to see such attacks combined with social engineering to either give the customer the impression that a specific payment has been initiated as intended or a payment has been erroneously received and should be reimbursed, or that access to online banking is not available for a certain time.

3.2.4.1 Suggested Controls and Mitigation

No dedicated controls or mitigations beside the ones listed against the social engineering and malware threats in section 2.

3.2.5 Payment Execution

Payment execution attacks refer to those attacks that focus on central processing systems where the actual validation of the transaction and the transfer of funds itself are executed. These attacks can occur at a bank or at an account information or payments initiation service provider, at a card processor, card issuer or acquirer network, as well as on a clearing infrastructure; attacks on SWIFT or other clearing interfaces fall under this latter scope. Such attacks may come with severe financial consequences, given that the impact from data losses, service disruptions or compromised transactions may be in the range of thousands up to billions of Euros.

Beside the DdoS attacks covered at large in the previous section, the greatest risk here comes from advanced persistent threat attacks (APTs). As explained in Section 2, they usually leverage themselves all possible techniques ranging from social engineering and DdoS up to specially crafted malware. There have been a wide diversity of APT attacks against financial institutions in the last years. Ultimately, they can target any entity, compromise whatever data, and misuse whatever service.

In the financial sector we have seen major data breaches primarily compromising bank card data. Targeted APT attacks have been conducted – most prominently – against SWIFT service bureau and gateway infrastructures but also against acquiring and card issuer authorisation systems.

In the following we give a brief overview of each one of these types of APT attacks.

Card data breach APTs

[47] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0546
[48] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0367

One of the first attacks involving the breach of cardholder data took place in 2004 where 40 million cards were compromised at the former company called CardSystems. Since then, many data breaches compromising many millions of cards have occurred and continue to occur. All these data breaches present various modus operandi following the structured approach mentioned in section 2.3.

The initial foothold Is usually executed through social engineering bank employees towards obtaining credentials, or by convincing the employee to open an attachment that will exploit a zero day vulnerability or by exploiting a vulnerability of an external facing system. Card data breaches vary in respect to the types of systems attacked and the types of data that they may harvest.

Compromise of databases holding card data continues to be common despite the enforced PCI DSS programs. These compromises have the characteristic of usually stealing data stored over various years and generally are limited to card numbers and expiry dates. It is not uncommon though, to also compromise CVVs as well.

Other data breaches intercept transaction data when being processed or whilst in transit in the communications realm. These attacks tend to compromise a shorter span of data given that they do not have access to historical transactions, compared to database compromises. On the other hand they usually compromise data of higher value such as CVV2 and chip or magnetic track data.

Some special variants of APT attacks consist in infecting terminals, POS or ATM with malware. These APT attacks go through the process of compromising internal systems and making lateral movements until they grasp a system with the capability of downloading software to the POS or ATM. In one case the malware on the infected POS was performing memory scraping getting the card track data and exfiltrating it back over the compromised internal systems. The reusable data is then typically sold in dark web forums and misused all over the world.

The adoption of EMV standards[2] based on chip cards has created a secure alternative to magnetic stripes, countering such attacks. However, the benefits of this new chip technology will only become fully effective with the complete ban of the magnetic stripe technology, at the basis also of magnetic stripe skimming and shimming attacks. These past few years have seen the largest missing countries adopting EMV, notably the US, so that cloned magnetic stripe cards can now solely be misused in the few remaining countries that have not yet embraced EMV.

SWIFT APTs

The SWIFT infrastructure has been designed with security considerations right from the very beginning and as an example of this commitment, protection of payment transactions is based on cryptography making use of hardware security modules. Even so, compromises have occurred where the operators and the SWIFT gateway systems that interface with operators and service users were exploited. This resulted in the injection of fraudulent transactions and specially crafted software that, in some instances, would even hide the fraudulent transactions from the operators.

SWIFT gathered intelligence with regard to these attacks and shared it with their customers under NDAs, so that customers can prepare specific mitigations against these kinds of attacks. Moreover, the SWIFT Customer Security Program has set forward a set of security requirements that SWIFT clients must adopt and get certified against. Very little information is publicly available about all

this except for the numerous attacks reported in the press and a substantial revealing report published by F-Secure[49].

Through the analysis of the various reported cases, it can be concluded that there are diverse modi operandi, however infecting bank or service bureaus' internal systems with malware is common to most attacks and the compromise of employee credentials is frequently one of the mechanisms used in these attacks. Most of these attacks have in common the fact that the time taken for attackers to prepare the final heist can be unexpectedly long, sometimes taking more than a year in preparation. On the other hand, the attackers manage to reap amounts ranging up to nearly a hundred million Euros.

Card Processing APTs

Some major attacks have occurred relating to the manipulation of card transaction processing parameters. Usually those attacks change the fraud control parameters, such as spending limits, of a few cards and then in a synchronized and distributed attack withdraw as much cash as possible in a timeframe of only a few hours.

As early as 2008, a major processor's systems were compromised and the attackers managed to replenish the available funds and raise the spending limits of 44 prepaid payroll cards. Three days later 9 million USD were withdrawn in 280 cities in a time window of 12 hours. Since this attack a few high profile attacks of the same kind have occurred: misusing a few cards to withdraw within only a few hours[50] [51] [52] many millions of Euro, on terminals spread all over the world.

Some of such attacks were the result of an APT laterally moving through internal issuer systems until the card processing system was reached.

3.2.5.1 Suggested Controls and Mitigation

No dedicated controls or mitigations beside the ones listed against the social engineering and APT threats in section 2.

3.3 Fraud unique to Specific Payment Instruments

The various threats and fraud patterns described in the previous section can basically lead to two categories of fraud, namely so called "Authorised payment fraud" and "Unauthorised payment fraud". *Authorised payment fraud* refers to authorised transactions in which the genuine payer initiates and approves a payment to an account under the control of a criminal. *Unauthorised payment fraud* refers to an unauthorised fraudulent transaction whereby the genuine payer does not provide authorisation for the payment to proceed and the transaction is carried out by a criminal.

The sections below describe fraud related to specific payment instruments.

---

[49] "Threat Analysis - SWIFT Systems and the SWIFT Customer Security Program" - https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-threat-analysis-swift.pdf

[50] "Eight Members Of New York Cell Of Cybercrime Organization Indicted In $45 Million Cybercrime Campaign" - https://www.justice.gov/usao-edny/pr/eight-members-new-york-cell-cybercrime-organization-indicted-45-million-cybercrime

[51] "Coordinated ATM Heist Nets Thieves $13M — Krebs on Security" - https://krebsonsecurity.com/2011/08/coordinated-atm-heist-nets-thieves-13m/

[52] "Indian Bank Hit in $13.5M Cyberheist After FBI ATM Cashout Warning" - https://krebsonsecurity.com/2018/08/indian-bank-hit-in-13-5m-cyberheist-after-fbi-atm-cashout-warning/

3.3.1 SEPA Schemes

The various threats and fraud enablers described in Section 2 of this document could lead to fraud on SEPA payment schemes (SCT, SCT Inst, SDD – Core and B2B) as well as on supporting schemes such as SEPA Proxy Lookup and SEPA Request-to-Pay. As set out in the previous section, regardless the payment instrument, the fraud can occur at all payment-relevant processes of a transaction.

These fraud scenarios are detailed in the next sections.

3.3.1.1 SEPA Credit Transfer (SCT)

SCT is a SEPA wide Credit Transfer scheme managed by the European Payments Council and its governing rules and standards are described in the SCT Rulebook.[53]

The following processes of SCT transactions can be targeted by various threats and fraud enablers:

On-boarding and provision

- A fraudster using various techniques, notably social engineering for asking for example a SIM-swap of a legitimate user mobile subscription, can open a profile and record a victim bank account. Once the provisioning is completed the fraudster may initiate fraudulent SCT transactions.
- A fraudulent, one-time access to account holder profile in an e-banking or mobile banking application, can be used to create fake beneficiaries. Recording these beneficiaries under genuine and known names, can trick the account holder when initiating SCT transactions. Also once a fake beneficiary is created, automatic and periodic SCTs can be configured so that at every term an amount of money is automatically transferred to the fraudster without further intervention by the victim. These fraudulent credit transfer transactions can be executed until the attack is discovered and can lead to important losses for the victim, often hard to recover as funds can be used for cash withdrawal, purchase of physical goods or for money-mulling purposes.
- Full fraudulent bank account creation (after identity theft or weak KYC procedures) for further use as Beneficiary account in fraud scenarios based on “money mules”.

Request-to-Pay and Invoicing

- These processes are not directly part of the SCT scheme. The payment using SCT scheme represents the “payment” part of a larger end-to-end purchase flow and is preceded by the invoicing or the RTP step. However, the RTP and electronic invoicing combined with payment are beneficial for payers as they facilitate smooth payment initiation without the need for entering transaction and beneficiary details. This advantage can be exploited by fraudsters to further automate the fraudulent actions leading to illegitimate fund transfers using the SCT scheme. Therefore Invoicing and RTP processes are relevant for the SCT scheme.
- The two main fraudulent actions with effect on invoicing and Request-to-Pay (RTP) processes have been described in the corresponding section of the chapter 3: Payee impersonation and IBAN manipulation. These are particularly relevant for the SCT scheme as the payment instrument most often associated with Request-to-Pay is Credit Transfer and this is for a large extent also true for invoicing.

Payment initiation and authentication

[53] SEPA Credit Transfer (SCT) Rulebook 2023 v1.0

- During the last years, the criminals' use of impersonation and deception scams, as well as online attacks to compromise data, continued to be the primary factor behind fraud losses related to SCT payments. In these methods, criminals target personal and financial details which are used to facilitate fraud or convince the genuine account holder to authorise a transaction to an account controlled by the criminal (Authorised Push Payment – APP).
- Various types of social engineering – detailed in Section 2 – can be used to initiate payments even if Strong Customer Authentication is active and mandated. Once the customer trust is obtained by these means, the fraudsters can make updates of the e-banking profile of the customer (mentioned in the Onboarding section above) or simply initiate credit transfers. According to the 2022 Fraud Report from UK Finance[54], intelligence suggests that criminals continue to focus on contacting customers by phone, text message or email pretending to represent a trusted organisation such as a PSP or the police, seeking to trick people into handing over personal details and passwords. Often the approach claims that there has been suspicious activity on an account, account details need to be updated or verified or a "refund" is due. The information gathered (such as passwords and passcodes, bank account details) are then used by the criminal to make an unauthorised payment. Criminals also use these fraudulent approaches to trick people into APPs. APP fraud is the fastest growing fraud in the UK and the related loss is even larger than fraud losses related to "unauthorised payment fraud".
- "Unauthorised payment fraud" is often the result of attacks using malwares. Malwares installed on the customers' devices (individual or corporate customers), or on the devices of bank agents in the bank's branches, to either intercept authentication credentials for further or immediate use on separate channels controller by fraudsters, or to directly initiate fraudulent credit transfers. According to ENISA Threat Landscape 2022[55], malware attacks increased again in 2022, after a decrease in 2020 and beginning of 2021.

Payment execution

- At the execution stage, once the customer is authenticated and a payment instruction has been initiated, sophisticated intrusions could target the PSPs infrastructures or infrastructures of the CSMs.
- An important technique that could be used now and for the future seems to be APT. It must be considered as a potential high risk not only for the payment infrastructure but for all network related ecosystems. With a limited number of criminals involved, a maximum result can be established (see Section 2.3).
- DdoS attacks, that can also rely on botnets can target PSPs or CSMs infrastructures can make serious damages and even if these do not have for object a fraudulent transfer of funds from customer accounts, they may create unavailability and affect the stability and the reputation of the payment operation infrastructures.
- In some cases, this type of attacks masks more classical attacks and is used to divert the attention and resource allocations of operational teams from actions of identifying and neutralising them.

[54] https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2022

[55] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

3.3.1.2 SCT Inst

SCT Inst is an "instant Credit Transfer" scheme managed by the European Payments Council and its governing rules and standards are described in the SCT Inst Rulebook[56].

The SCT Inst scheme can be impacted by the same threats and fraud enablers, and at the same stages of processing, as the classical SCT scheme. However, SCT Inst has specific features that distinguish it from the SCT scheme and that can be exploited leading to specific fraud:

- An SCT Inst transaction is much faster than an SCT transaction. The originator account is immediately debited, and the funds are instantly made available on the account of the beneficiary. It is executed in seconds and therefore the following consequences can be expected:
  - Whilst at the initiation and authentication stage, the fraud techniques based on *social engineering* and *malwares* are performed in the same way as for SCT, initiation is immediately followed by the execution and the use of funds fraudulently received is immediately possible for cash withdrawal or physical purchases.
  - The overall speed of transactions to/from "*money mules*" is much higher so that this type of enabler/monetisation channel is expected to be more intensively used with SCT Inst.
  - At the execution stage, the mechanism for fraud detection and transactions blocking must be executed in real-time.
- SCT Inst transactions must be processed continuously, on a 24/7 basis so that it is not possible to use the time before batch processing to perform anti-fraud screenings.
- The clearing and settlement is executed in almost the same time as the payment orders so that disruptions caused by *APTs and DdoS* might also affect these layers of transactions.

3.3.1.3 SDD (Core and B2B)

SDD Core and SDD B2B are SEPA wide Direct Debit schemes managed by the European Payments Council and their governing rules and standards are described in the SDD Core and SDD B2B Rulebooks[57].

The following processes of SDD schemes can be targeted by various threats and fraud enablers:

On-boarding and provision

As in both SDD schemes the payment transactions are "pull" mode transactions (debtor account is debited on the basis of a debit/collection request coming from the creditor – provided that a proper mandate is signed by the debtor to allow the creditor to initiate such transaction), the on-boarding stage concerns the creditor. Moreover, on-boarding a creditor in an SDD scheme require a strong KYC process on the creditor PSP side. Although it might be possible that a fraudulent entity requests from a PSP to become a creditor in an SDD scheme, there were no notable fraud attempts of such type in the last years.

This would require that representatives of the fraudulent company be able to trick the controls that banks perform when registering companies for the role of SDD Creditors. For this type of fraud to happen, one would have to make use of complex *social engineering* targeting the corporate customer services of PSPs.

---

[56] SEPA Instant Credit Transfer (SCT Inst) Rulebook 2023 v1.1

[57] SEPA SDD Core Rulebook 2023 v1.0, SEPA SDD B2B Rulebook 2023 v1.0

If the signature of the SDD mandate by a debtor is considered as part of the on-boarding process, another type of fraud is that the debtor indicates on the SDD mandate an IBAN of an account that does not belong to that debtor. A fraudulent debtor could in this way benefit from goods and services paid by SDD, whilst the payments for these services and goods are executed from someone else's bank account. The scheme's rules however allow the victim to require the refund of amounts so that the effects of this type of fraud on the debtors can be easily mitigated.

Some merchants (e.g., selling digital goods, subscriptions to digital services, parking, subscriptions to newspapers and magazines etc.,) do not require a wet signature or the equivalent of the mandate and instead propose customers to sign a mandate by answering to an SMS, checking an option on a web portal, or sending an email containing an account number. Even though, depending on the jurisdiction, these forms of expressing an agreement are legally valid, the possibility of abusive use by some merchants could lead to fraud through *social engineering*.

Request-to-Pay and Invoicing

When starting a long-term, recurrent, commercial relationship merchants and service providers may propose customers to pay their invoices by Direct Debit. Often the mandate proposal is attached to the first invoice regardless if it is in paper or electronic format.

Wrong or unclear formulations in the mandate, identity theft, misleading presentation of the mandate scope could all be leveraged as *social engineering* towards convincing customers to sign valid SDD mandates for fraudulent purposes.

Initiation and authentication

In SDD schemes, the payment is initiated by the creditor. It is of the responsibility of the creditor PSP to ensure proper authentication of the creditor for the execution of direct debit collections. Nevertheless, it is neither in the SDD scheme rules, nor can it be in the authentication processes that the SDD mandate is verified. Therefore, there is a risk that a fraudulent creditor tries to execute SDD payments by debiting victims' bank accounts without a mandate.

According to the 2022 yearly report from the Banque de France's Observatory of the payment instruments' security, this was the main fraud technique used in 2022 in France for SDD fraud[58].

Another type of SDD fraud is based on the complicity between a fraudulent creditor and a debtor. With a proper mandate the creditor regularly debits the debtor's account increasing the amounts. A short time before the end of the 13-month period for legal refund, the debtor contests the payments and asks the refund to their bank. At that moment, the creditor had transferred the funds to another account or transformed them in cash so that the creditor bank cannot recover these funds but is obliged to refund the debtor bank which had refunded the debtor.

It has to be noted that the SDD B2B scheme is less likely to be targeted by fraud than SDD Core, as in SDD B2B the debtor is always a company and it is required that the debtor PSP verifies each collection to ensure that it is authorised under the mandate.

3.3.1.4 Supporting schemes

SEPA supporting schemes can be defined as schemes covering the exchange of the data necessary to initiate payments and facilitating interoperability.

[58] https://www.banque-france.fr/fr/publications-et-statistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2022

Currently the EPC manages two supporting schemes: the "SEPA Proxy Lookup Scheme" (SPL), and the "SEPA Request-to-Pay" (SRTP) messaging scheme. The version 3.1 of the SRTP Rulebook was published in May 2023[59].

Potentially when targeting supporting schemes, all relevant *payment related processes* that were detailed in Section 3 can be affected by some *threats and fraud enablers* set out in Section 2. Nevertheless, as the supporting schemes are relatively new, it is too early to observe specific real-life fraud actions targeting them.

3.3.1.5 Suggested controls and mitigations

Fraud prevention for SEPA schemes requires measures that involve all actors in the payment chain and are applicable to all payment processes. As part of its Scheme Management role, the EPC provides for each scheme, a Risk Management Annex (RMA), complementing the schemes Rulebooks. These RMAs are made available to scheme participants (PSPs) and include the identification and evaluation of risks and measures for their mitigation aiming to ensure an adequate degree of security, operational reliability and business continuity for the concerned scheme participants and their customers.

Regardless the scheme, some measures and best practices are:

- Establishing secure communication channels that guarantee data integrity and confidentiality, and mutual authentication between PSPs and Clearing and Settlement Mechanisms (CSMs)
- Use of appropriate measures against DdoS attacks on PSPs' and CSMs' platforms
- Implementation of adequate fraud monitoring systems; regarding the SCT Inst scheme, these systems should be able to perform real-time analysis and related actions, due to the instant characteristics of this scheme
- Secure connection from/to the originator and beneficiary devices (PCs, mobile phones) and the corresponding PSPs
- Use of Strong Customer Authentication (applicable to SCT and SCT Inst) with dynamic linking with Beneficiary identifier and transaction amount
- Promotion of security and data protection awareness, training and education wherever possible including warnings for phishing attacks, and encouragements to adopt security measures on the customer devices.
- Regarding SDD schemes (Core and B2B), the creditors should ensure the protection and authenticity of the mandate given by Debtors.

Other measures fall under the scope of supporting schemes such as SRTP or SPL. For example, among measures specific to the SRTP scheme, the following could be mentioned:

- RTP Service Providers, especially when these are not regulated entities (non-PSPs), should complete a proper homologation process as part of the scheme onboarding stage. Indeed, PSPs should have certainty that the processed Requests-to-Pay are valid and originate from a legitimate scheme participant.
- Payees need to be legitimate and accepted as customer of SRTP Scheme participants upon completion of agreed customer authentication and identification procedures. Indeed, SRTP scheme participants (and ultimately payers) should have certainty that received Request-To-Pay (RTP) messages = are valid (i.e. created by a legitimate payee,

[59] SEPA Request-To-Pay (SRTP) Scheme Rulebook v3.1

contain valid payment-related data like amount/payee IBAN and represent a real business transaction).

3.3.2 Card Scheme

Card based transactions have historically been very successful due to the acute balance between security and convenience in authenticating these transactions through the card magnetic track (something you have) and the PIN (something you know).

In the late nineties fraud trends started to explore the fact that the magnetic stripe became quite easy to clone and thus led to the adoption of the EMV chip card to substitute the magnetic stripe.

Meanwhile with the emergence of the internet, card number based payments started to be accepted but opening up to new avenues of fraud. Several mechanisms were adopted along the years to secure theses transactions namely the adoption of the CVV2 and the adoption of 3-D Secure protocol.

In the 2010's contactless cards started to surge building on the fact that chip cards were capable of computational processing and so could support yet the processing through this new interface.

In recent years mobile devices have the capability of implementing contactless transactions by emulating the contactless card through NFC (Near Filed Communication) technology.

As a result of the application of PSD2 RTS on SCA ([2]), all European payments benefitted of higher levels of security. Magnetic stripes on bank cards were, for acceptance purposes, still accepted as a fallback until the compulsion of SCA in September 2019. Meanwhile internet card payments force SCA through the 3-D Secure protocol that has evolved to a second version that enables frictionless and better authentication across devices. It also supports more information to determine the risk of the transaction.

In general, the fraudster's *modus operandi* is to obtain the physical payment card (or card data) and PIN for use in a face to face, Point of Sale (POS) or ATM environment. Alternatively, to obtain payment card data for use in an e-commerce or card not present (CNP) environment, such as Internet shopping, mail order, phone ordering, etc. – if the card supports this functionality. Lately, omni-channel fraud e.g. using stolen card information from social engineering in wearables and mobile devices in a POS environment has been increasing, as well as fraud cases where both SEPA-schemes and card payments are being interlinked and used as combined vehicles to move stolen funds and handle the exfiltration of crime gains.

The adherence to PSD2 has changed the attack context and a trend to the adoption of social engineering attacks has been observed, as a way to circumvent the adoption of SCA. Below are the most common, as well as new, fraud trends within the card present and card not present space.

3.3.2.1 Card present

Card present fraud is a wide-ranging term relating to the theft and crimes committed using or involving a payment card, or other tokens with card details in physical POS terminals or ATMs. The purpose may be to obtain goods or services to resell for cash or to obtain funds directly from a related payment account.

Lost and stolen card fraud

Fraudsters consistently look at better and easier ways to capture PINs, e.g. using social engineering or shoulder surfing, and then stealing the payment card using one of various methods, often targeting the elderly or the uninformed. In this way, getting the card and the PIN to execute real payment transactions is often hard to detect.

Contactless payment cards are being increasingly accepted in stores. A lost or stolen card can be used for purchases as long as the cardholder authentication (PIN, CDCVM) is not required for a contactless transaction at POS terminals, but only up to a certain number of transactions and/or to a limited value. It is expected that there will be an increase in the theft of cards for this purpose, i.e. to purchase goods that can be easily resold for cash. ATM cash transactions always require a cardholder authentication thus are not subject to this attack scenario.

Another fraud type to consider is card-not-received fraud, that takes place when a criminal steals a payment card from an individual's mailbox or in the mail delivery process, so the rightful owner never receives it. This type of fraud is only effective when the card is delivered in an active state. It should be noted that most card issuers issue inactive cards, that can only be activated by the genuine cardholder. By doing so, cards intercepted in the delivery process will be of little or no use to the attacker for card present transactions.

Contactless cards intercepted in the delivery process will not transact until a contact online transaction is performed and so mitigate the risk of an attacker performing contactless transactions that do not require cardholder authentication.

Account take over / Fraudulent cardholder application.

Fraudsters are using social engineering techniques such as doing visits to cardholders' homes, approaching PSP staff or other methods, such as spear phishing, to obtain the data needed to take over an account or create a false cardholder application / request for a payment card or PIN.

Counterfeit and skimming

Copying magnetic-stripe track data at POS terminals and ATMs by skimming is an ever-diminishing type of fraud in Europe.

With the compliance of PSD2, magnetic stripe-based transaction of European cards on European terminals, were forbidden. However, the so-called one-legged transactions, where either the card or the terminal are non-European, magnetic stripe-based transactions may be accepted.

Protecting terminals from skimmers has proven to be challenging at most. Skimmers have evolved from classic external skimmers to non-metallic skimmers, stereo analogue skimmers, and lately to inlay and insert skimmers. PIN capture has been enabled through PIN pad overlays or through ever-smaller spy cameras.

Magnetic stripe cards cloned with the stolen card data may be used on terminals where EMV chip technology is not supported or required. While usage of such cloned magnetic-stripe payment card cannot be used in the European area, this is still possible in countries where EMV has not yet been fully introduced, hence fraudulent usage, namely cash-out, is often performed outside of Europe.

Shimming – like skimming, is where the aim of the fraudster is to skim or 'shim' data from the EMV Chip on a payment card rather than from the magnetic stripe, using similar methods. Criminals can exploit this when issuers have implemented the EMV protocol incorrectly. Some attacks making use of skimmed and shimmed data has been observed coming from out of Europe namely doctoring all types of data in the messages trying to explore failures in the issuers processing implementation.

ATM fraud

ATMs are also vulnerable to several other attack vectors, not limited to, but including physical attacks, malware/logical manipulation, black box attacks, jackpotting, card and cash trapping, etc. Black box attacks observed a rise in European ATMs since 2020. Malware designed specifically developed for ATMs continue to occur throughout the world.

ATM MitM and relay attacks have been observed recently in several European countries. These attacks intercept communications between the EMV chipcard and the ATM and relay this information to another ATM (rogue ATM), where the attacker is at. The victim will be unaware to the fact that the card inserted in the ATM is dialoguing with another ATM through a shimmer and communications equipment relaying the card commands and responses back and froward. The PIN will have to be equally captured and transmitted, typically by streaming video to the attacker that will type it in at the rogue ATM. Meanwhile the ATM where the victim is operating will have to be fooled into taking the transaction forward, including requesting the PIN introduction, but should be led to abort the transaction so as to avoid the ATM transmitting the transaction to the processor.

For more insights on ATM-related fraud and attacks, please revert to the bi-annual report produced by EAST (European Association of Secure Transactions).

First party fraud (overdrafting credit limits)

Non-credit worthy people trying to get payment cards and banking accounts with the only purpose to overdraw the accounts / credit limits without any intention to pay back. The only interest is to overdraw to get cash and/or to purchase goods/services. Usually a weak KYC procedure and too flexible card products provided to the customer with generous credit limits are causing first party fraud.

Friendly/Family fraud

Friendly fraud occurs where a victim's relative or acquaintance performs transactions without the knowledge of the victim. This kind of fraud usually involves non-significant amounts but usually is complex to investigate and requires significant effort.

Merchant refund fraud

This fraud occurs when the fraudster, through different methods, hijacks an in-store card terminal and uses it to make refund purchases with stolen cards. To make sure the merchant has sufficient funds on their account, the fraudster often first makes purchases using stolen cards. They then cash out in ATMs immediately afterwards. The fraudster has knowledge about terminal functionality and can in some cases also have inside help at the targeted merchant. This type of *modus operandi*, according to multiple sources e.g. Mastercard, had an increase during the Covid-19 pandemic, given that the genuine flow of refunds increased due to cancelled services and events.

Shell companies and fake merchants

It has been noted that criminals set up fake, or bought existing non-active corporations, and used these to sign card acquiring agreements in order to accept card payments that will be later used to exfiltrate funds. These *modi operandi* are often complex and are performed in several steps, from setting up the corporation, acquiring info on the target, creating a good cover story for the social engineering to exit with the illicit gains.

3.3.2.2 Card not present (CNP)

Card not present fraud is a term relating to the theft and crimes committed using or involving payment card credentials for making authorized or unauthorized purchases in the e-commerce space, MOTO or other instances where the physical card is not involved in the process. The purpose may be to test the validity of the credentials, to obtain goods or services to resell for cash or to obtain funds directly from a related payment account.

Unauthorized card not present fraud

As the volume of payment card purchases made via the Internet continues to grow, so too do the attempts of Card Not Present (CNP) fraud. E-commerce is the preferred way to buy goods or services where the payment card is not physically present, and stores must rely on the cardholder information indirectly. Payment card details are obtained by fraudsters in various ways: by malware, data hacks, phishing or fake merchants stealing the information. This information is later sold on criminal marketplaces on Darknet/Deep Web, to be used by other fraudsters, or sometimes used by the bad actors stealing the credentials themselves. The modus operandi for committing the CNP-fraud is normally either through large volume automated algorithmic attacks on well-known e-commerce websites, trying to hide the fraudulent transactions in the vast volume of legitimate transactions, or by using the credentials more diligently for single high-amount purchases on selected merchants or merchant categories. A common modus operandi adopted by cybercriminals is to try to extrapolate card numbers, including expiry dates and sometimes also CVV. They then use those generated numbers for large scale BIN-range attacks involving low amounts and when they get a hit they make use that card on a high amount transaction to purchase easily transactional goodsBelow are the most common ways for criminals to access card details.

Account Data Compromises

ADC attacks are targeted at specific stores, financial institutions, services providers or other sites holding valuable card or customer information in their databases, with the aim to compromise the network or payment system and gain payment card data.

Everyday tens of vulnerabilities are published, usually relating to widely adopted software. Some vulnerabilities are called zero-day vulnerabilities given that at the time of disclosure no patch exists for its resolution. It is typical for small merchants not to have the necessary awareness or resources to prevent and maintain secure environments for the processing of card data given that security is not their main focus.

In connection with the above, hotels, online tour operators are currently, and historically, responsible for a large part of the stolen card data. Card data is stolen in transit or in data storage, and it results in various sorts of unauthorized CNP-fraud.

Although these attacks can occur on any payment systems there have been attacks against payment card issuers resulting in serious fraud losses. Payment cards with an almost infinite limit are issued by the fraudsters and intercepted, duplicated and distributed within their global fraud network. Attacks are organised and occur mainly during periods when fraud monitoring is at a low level, e.g. at night or during weekends. After penetrating a system, fraudsters can sometimes wait for months, ‘sleeping’ inside the system before completing their attack.

Card generation, testing and harvesting

The objective of this attack is for the criminal to acquire knowledge on the existence, status or other sensitive information related to accounts. For example, in a testing attack a malicious actor

may try to test if a card PAN exists, test CVVs or expiry dates related to a certain PAN or try to inject any transaction with doctored fields to try to fool the authorisation system in accepting the transaction as valid.

These attacks can be performed through the transaction authorisation systems or even through the ACS enrolment verification systems. Account testing attacks can harvest millions of card credentials if no fraud detection system is in place, with the capability to intercept transactions. Attacks have been detected where accounts are tested at great speeds (up to 12 per second).

Testing the accounts can be performed on certain merchants that do not have mechanisms in place to detect these kinds of attacks and once the elements are all known, the attacker can perform high value transactions on unsuspecting merchants.

Simple Account Take Over

A cardholder enrols to a payment page on a merchant's website who has a secure storage solution (PCI compliant or equivalent) of card data on file. The loading of card data on file occurs with or without 3DS. The access for making payments on the merchant site is sometimes through a simple cardholder ID and password, chosen by the cardholder. In this case a fraudster can find out about these credentials and subsequently make payments using the cardholder's secured card-data-on-file, after possibly changing delivery address, service to be delivered etc.

Digital skimmers

Malicious code is increasingly being injected into websites catering for the payment process at various e-commerce merchants. The code can identify the card and customer credentials, provide them to the criminal and later resolve itself to avoid detection. The Magecart groups responsible for this are highly active and are behind several noticeable incidents.

Fake merchants

A huge source for stolen card credentials, is the increasing number of fake merchant websites that can offer anything from high end consumer goods to gift cards or freight deliveries. They often work through social media advertisement, phishing e-mails or text messages. Even if the card holder's authorised or not authorised card payment is declined by the issuer's preventive measures, the actors behind the fake merchant still apprehend the customer and card credentials, to later be used for various fraudulent attempts.

Authorized fraud and scams

With more SCA solutions in place all over Europe, this type of card not present fraud is increasing and expected to increase even more as the related requirements of the PSD2 ([1]) and the RTS ([2]) legislation get implemented. Basically, the fraudster goes after the weak link in a SCA payment chain, which often is the human. You could normally split this modus operandi in two main tracks, both often initiated via some sort of phishing:

- *Identity theft.* The fraudster steals or tricks the victim to disclose their card/personal credentials/online banking verification methods and thereafter make the transaction, often to money mule accounts. Here we also have seen a recent problem with Global Wallets for contactless or e-commerce payments. If the card issuer does not have strong enough enrolment and card credential provisioning solutions, this service can become a vessel for social engineering fraudsters who download wallets into their own mobile devices and can perform fraudulent SCA-transactions. In many of these types of fraud the entry point towards the victim consists of different forms of phishing/vishing/smishing obtaining the online banking credentials and the exit of money is with card payments.

- *Authorised card transaction scams.* In this case the fraudster persuades the card holder to perform the transactions themselves, either by impersonating to be someone/something else or by selling fake services or goods. This fraud can be very devastating for the victim since they are not always refunded in view of unclear definitions of fraud and related liability. There is also often a personal shame in being scammed like this, hence the hidden number of victims can be big. Examples of authorised transactions fraud where card payments are used include investment fraud, romance fraud, phishing sms/e-mails leading to fake websites, fake purchases of goods turning into unwanted subscriptions, fake advertising for renting apartments etc. Recently, more elaborate spear phishing techniques has been seen to a greater extent, where the fraudster has spent time for background checks and in various ways create a more plausible story for the victim to believe when they are approached, e.g. pretending to be from the card issuer security department or the police.

3.3.2.3 Suggested Controls and Mitigation

For Merchants and acquirers:

- 3D Secure: security protocol to authenticate users for payment card transactions in card-not-present scenarios. 3DS version 2.x has enabled the possibility for the merchant to pass extra data to the issuer. This data supports risk-based authentication maintaining the transaction as frictionless as possible, and should be used for fraud detection systems
- Tokenisation: process of substituting sensitive data with a non-sensitive equivalent called token. By doing so the risk related to an eventual data compromise is reduced and so too liability.
- Fraud monitoring. Deploy a responsive, real-time fraud system with prevention capabilities that identifies suspicious patterns of behaviour.
- Patch vulnerabilities and adopt recommendations Always use the latest recommended update and recommendations for the operational systems from service provider, card schemes, etc. Always patch systems when needed.
- Perform an annual risk assessment by your Security, Risk and / or Fraud Departments to check if all mitigating measures are completely set and in control.
- Educate store employees on how to identify and how to act when they suspect fraudulent behaviour in POS-environment. Make sure to have well working routines to alert and how to protect the cash register and card terminals.
- Store and process customer data according to PCI DSS standards (if the respective card scheme adheres to this standard). Restrict the number of places where card data is stored and processed to a minimum. If possible, do not store card data in your own environment, rather let the payment gateway or service provider do that.
- Make sure that the customer onboarding process when signing new card terminal agreements, is robust and performs a diligent KYC to avoid bad actors getting into the system to be able to accept card payments for illicit purposes.
- In order to mitigate relay attacks, tweak the timeouts to trim excessive chip card response times.
- Check integrity of card data whenever possible so that magnetic stripe, chipcard and contactless data are consistent between themselves.

For Card Issuers:

- Inform cardholders of the contact channels for reporting lost and stolen cards or any detected suspicious fraud situation.
- Provide means for the cardholder to consult bank statements in order to facilitate the detection of illegitimate transactions.
- Geo-blocking: To protect payment cards from being misused by skimming fraud, it is strongly recommended to protect payment cards within a geographical region of use.
- Restrictions and blockings: To limit the usage of payment cards to specific channels or specific contexts according to the Issuer's defined risk appetite.
- Offer virtual cards that will have lowered spending limits, shorter validity periods or restrictions on the merchants where they may be used.
- Adopt Strong Customer Authentication (SCA) with every aspect of the payment card and PIN replacement.
- 3D Secure: security protocol to authenticate users for payment card transactions in card-not-present scenarios. 3DS version 2 .x should be adopted given that the extra data passed on from the merchant to the issuer will allow a risk-based authentication maintaining the transaction as frictionless as possible.
- Card synchronisation in stand-in systems. Some stand-in systems have no knowledge of what cards exist and are active (they only know of the ranges of cards that they process) and therefore the capability to detect account testing attacks is greatly reduced so too is the capability to protect against brute force attacks.
- Non-sequential issuance of cards. Some issuers still issue cards in a sequential manner. Thus, all cards in a certain range will be valid and with the same expiry date. In order to reduce the level of success for an attacker to determine valid PANs and also in order to help fraud detection systems, PANs should be issued in a non-sequential fashion. By doing so, an attacker that sweeps through a range of PANs, will generate a high percentage of "Inexistent PAN" errors and ultimately be detected with greater ease.
- Card limits: Allow for easy access customer customisation of ATM withdrawal limits, daily spend, e-com environment and contactless functionality, possibility for temporary block in mobile bank app etc. Promote customer awareness on this.
- Transaction information: Inform your cardholders about authorised transactions in real time (could be SMS or push messages) to enable quick customer feedback.
- Perform an annual risk assessment to check if all mitigating measures are completely set and in control.
- Besides the technical measures, awareness-raising (customer education) is an essential point to prevent, more in particular, "low-tech" fraud.
- Work together, non-competitively, with other players and law enforcement agencies within your market to establish good communication lines and information sharing forums. Use these forums for mutual information sharing and raise awareness to customers.
- Make sure your Fraud and Chargeback team works closely together and with resources and tools available to identify the growing problem of friendly fraud.
- Within your local market, engage in working with others to develop standardised digital identification methods for safer e-com purchases and online access to bank account information.

- Make sure no credit limits can be overdrawn in any offline environment with your issued cards. Perform a diligent credit underwriting process.
- Make sure no offline limits can be reset by card holder actions to commit friendly fraud.
- Global Wallets – Employ an enrolment solution with Strong Customer Authentication to heavily reduce the risk of fraud.
- Fraud monitoring: Use a multi-layered approach from authentication to authorisation, which includes automatic customer interaction. Deploy a responsive, self-learning, real-time fraud system with prevention capabilities and risk scoring. Ensure your fraud system identifies suspicious patterns of behaviour to stop fraud based on both generic and tailor-made scenarios and rules.
- Geographically incompatible fraud rules are quite important to detect card present transactions that are impossible to be performed given the excessive velocity necessary to perform both transactions. This is quite useful to help detect some relay attacks such as the ATM MitM and relay attack.
- Deploy mechanisms and intelligence designed to proactively identify breached, leaked and skimmed card credentials with the purpose of taking action such as card exchange or dedicated monitoring on specific at-risk cards.

For Cardholders:

- Always keep your payment card in a safe place and protect your PIN. Report immediately to your card issuer, if the payment card goes missing.
- When typing in your passwords or PINs, especially in public environments, shield the typing from rogue cameras or eavesdropping attackers, with your hand or body.
- Do not give away your personal information or codes to your identification method if you do not initiate the event yourself.
- If a financial institution offers controls on limits and e-com and contactless functionality for the payment card, ensure you set these at the settings typical for your daily usage.
- If your financial institution offers geo-blocking, set the correct geographical region of use and adjust it on time for your convenience.
- Always check with your card issuer first if you receive suspicious information or requests via SMS/mail/telephone to initiate a log-in procedure or approve a transfer. The issuer never requests the cardholder to do that. Fraudsters typically press on the urgency for the victim to act fast, which is also not how banks and issuers communicate.
- Avoid to store your card credentials “on file” at an e-commerce merchant. But if not, make sure that you understand what type of payments can be made, and who is able to initiate a payment with your card.
- Always stop and challenge if a social media advertisement is too good, an offer seems very lucrative or if someone tries to talk you into investing in a once in a lifetime opportunity. Check with your issuer or bank first and talk with a family member or friend to assess the situation in a calm way.

3.3.3 Mobile Payment Wallets

A mobile wallet is a service accessed through a mobile device, which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications. This service may reside on a mobile device owned by the consumer (i.e. the holder of the wallet) or may be remotely hosted on a secured server (or a

combination thereof) or on a merchant website. Typically, the so-called mobile wallet issuer provides the wallet functionalities, but the usage of the mobile wallet is under the control of the consumer and his mobile device. Mobile wallets are frequently used for m-commerce.

Innovations in mobile payment options facilitate adoption of the technology by consumers and businesses, but also increase the interest of fraudsters to steal money, payment card information or history of operations.

Mobile wallets like all other payment types are exposed to the generic payment process relevant attacks mentioned in Section 3. There use cases may include contactless and card-not-present in-app e-commerce payments, but may also be based upon prepaid accounts or cover for person-to-person payments. By the fact that implementations are typically all virtual, mobile wallets supporting card payments generally leverage some type of card tokenization and with this also take advantage of the security add-ons that tokenization offers over physical cards. Nevertheless, mobile wallets also introduce new threats and third-party dependencies worth taking a closer look in this section.

Mobile payment wallet specific threats

In order to best possibly leverage today's mobile user experience and mobile device support for biometric authentication, card schemes encourage wallet providers to support **Consumer Device Cardholder Verification Methods (CDCVM)** instead of traditional CVMs like PIN@PoS (Point of Sale) or signature.

What this means from an ecosystem perspective is that

(i) terminals cannot work offline anymore with cards proposing CD CVM in contactless transactions (there is no plastic card anymore to support classical CVMs)
(ii) card credentials cannot be protected by certified payment chips anymore (there is no payment chip as those wallets exist only virtually on a mobile phone or server)
(iii) issuers cannot authorise transactions on the basis of a PIN securely entered at a POS anymore (as PIN entry and verification are substituted by CD CVM on the mobile device).

In summary mobile wallets thus come with a significant increase in user experience at the cost of a new ecosystem setup, in which Original Equipment Manufacturers (OEMs) and wallet providers often take over a large part of the security set-up without taking over its associated liability.

As a matter of fact, security largely differs between mobile device types and wallets. CD CVM credentials may be biometric, possession- or knowledge-based and card keys or tokens may be hardware or software protected. Moreover, mobile wallets may confirm a successful CD CVM based authentication to the card or token issuer on the basis of a device being unlocked at the time of payment initiation or may require an on-purpose validation of a device unlock credential or a wallet-specific authentication means.

Specific threats in the mobile wallet and CD CVM space include targeted attacks on mobile device key stores, unlock credentials, user interfaces and NFC controllers. All of these may get exposed through malware leveraging privilege escalation or rooting / jail-breaking exploits. Although mobile devices come with inherent security like secure boot and app signing and sandboxing, drive-by privilege escalations attacks keep on being reported across all operating systems.

Particularly worth mentioning in the mobile wallet space are **NFC relay attacks**, whereby a card on the cardholder mobile device can relatively easy get exposed to contactless payments on a fraudster device. But also other **mobile device interface attacks**, in which a fraudulent app

remotely exposes the mobile device user interfaces (display and/or touch input) or tricks a user in submitting his device's unlock credentials for a fake purpose (e.g. fingerprint for health checking) pose new threats. While there is first evidence from EAST about relay attacks happening in the wild, interface attacks have been observed at various levels for a while. An illustrative example for remote exposure of user interfaces is the accessibility interface attack formerly observed against a well-known payment processor[60] but also the very recent new attacks by the Vultur RAT[61]. Worth mentioning are also **physical attacks against biometric authentication implementations**, be it through copying fingerprints from the touchscreen or exploiting biometric sensor implementation weaknesses[62].

For a high-level coverage of mobile application user, mobile device and digital wallet application threats, the ENISA report from 2016 on the 'Security of Mobile Payments and Digital Wallets[63] still remains a good reference, listing the following threat categories:

- Phishing and social engineering
- Installation of rogue applications and malware
- Unauthorized access to lost or stolen mobile device
- Malware installation on the device
- Reverse engineering of the application source code
- Tampering with the mobile payment application
- Exploit of mobile payment application vulnerabilities
- Installation of rootkits/malware
- Mobile Operating System Access Permissions

3.3.3.1 Suggested Controls and Mitigation

Segregation mechanisms like Trusted Execution Environments (TEE) but also privilege escalation detection and remediation mechanisms like root-kid detection or secure device boot today represent inherent mobile platform security features that together with regular OS updating lay a strong security foundation for mobile wallet implementation. However, as they regularly also show exploitable software bugs and network providers at some point in time block OS updates for older devices, the security of CD CVM must independently be assured.

An EMVCo document[64] covers for both 'CD CVM best practices' and 'CD CVM security requirements'. While the security requirements document comes with a very comprehensive risk analysis and specific CD CVM attacks and countermeasures, the best practice document states the following general security-related recommendations that give a good insight to the challenges encountered and worth controlling in this rapidly growing third-party dependency space:

- Do not set a dormant value (factory-set default Reference Data) for a CD CVM Solution
- Warn the user when prompting for consumer authentication if the device is not in the appropriate secure state.

---

[60] https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

[61] https://arstechnica.com/gadgets/2021/07/new-bank-fraud-malware-called-vultur-infects-thousands-of-devices/

[62] https://www.computing.co.uk/news/3082909/natwest-nationwide-samsung-fingerprint

[63] https://www.enisa.europa.eu/publications/mobile-payments-security

[64] https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/CDCVM-statement_FINAL.pdf (the document is in the members' area of the EMVCo website, credentials are needed to access it)

- Prolonged authentication should not extend beyond a reasonable period of time.
- If the conditions for persistence are broken, then re-authentication must be performed.
- The number of incorrect CD CVM attempts should be limited.
- Do not allow weak CD CVMs
- Manage the lifecycle of a CD CVM appropriately
- Biometric modalities should not allow the registration of too many of those same modalities.
- The platform should provide a means for a Mobile Application to determine whether a suitable level of consumer authentication is active for the device.
- The fall-back/primary CD CVM should be sufficiently strong.
- For a biometric, there should be a balance between allowing the verification of the incorrect biometric and not verifying the correct biometric.
- There should be a mechanism for liveness detection and the ability to spoof the solution should be minimised.

To support these objectives, EMVCo has established a Security Evaluation Process to help ensure CD CVM solutions maintain certain minimum levels of security, including mechanisms and protections designed to withstand known attacks.

4 Conclusions

The main attack focus over the past year has continued to be the trend of shifting away from malware to social engineering attacks. Social engineering attacks, phishing and vishing attempts are still increasing and they remain instrumental often in combination with malware. Whereas in the past consumers, retailers and SMEs had been the main focus, the last year more and more company executives, employees (through CEO fraud), financial institutions and payment infrastructures appear to become preferred targets.

Malware remains a major threat but more particularly ransomware has become the top cyber threat faced by European cybercrime investigators. This type of attack appears to be more profitable to the attackers than the traditional banking Trojans. It is not possible to achieve full protection to not be hit by a malware attack. However, raising awareness campaigns with a few simple advices to customers to mitigate malware attacks (software updates, anti-malware tools, do not click on links, etc.), is one of the best tools to mitigate the risks and their impact. Similar awareness must be in place for the employees of PSPs.

One of the most lucrative types of payment fraud now and for the future seems to be Advanced Persistent Threats (APTs). It must be considered as a potential high risk not only for the payment infrastructures but also for large customers, including merchants

The number of DDoS attacks remains high and they are still frequently targeting the financial sector and have impacts on the availability of their services to customers.

There is a continuation of botnets and because of the high volume of infected consumer devices (e.g., PCs, mobile devices, etc.) severe threats remain. Besides an ever-increasing level of professionalism among the attackers whereby addresses of infected computers, routers or bots are sold or rented, the usage of IoT devices (such as CCTVs) for launching DdoS attacks have continued to be noted. It is expected that the usage of these devices to launch attacks will further increase over the years to come.

Supply chain attacks are important for PSPs that rely on third-party vendors. Until now, no incident has significantly impacted PSPs, but third-party vendors are more and more critical. Moreover, there are examples that illustrate the potential impact of these type of attacks. PSPs should therefore carefully assess its dependencies on third-party vendors.

Mobility is part of both consumers' and enterprises' daily life and operation. Smart mobile devices have become commonplace in Europe enabling a wide variety of mobile apps, including payment apps (see Section3.3.3). As a result, they are more and more becoming an attractive target for cybercriminals and fraudsters.

The need for reducing operational costs and the huge and rapidly growing amount of data lead to new business decisions for adopting cloud and big data analytics technologies. Data everywhere, "data in flight", data produced and stored in billions of interconnected devices, data in the cloud, and new technologies are bringing new opportunities to businesses but new risks too.

There is also a competitive market drive for user-friendliness and simplicity which leads to increased pressure on security resources and difficult trade-offs to be made by PSPs. The challenge will be to find the right balance between the user-friendliness and the security measures needed. As security becomes more regulated (PSD2 [1] and the RTS [2], NIS Directive [3], GDPR [4]), payments also face a new regulatory landscape in Europe, which on one hand increases the security barrier with respect to fraud (e.g. strong customer authentication) but at the same time also "opens up" the payment value chain which introduces new security challenges for all stakeholders involved.

Concerning card payment fraud, as long as mag-stripe is still largely usable in some countries, counterfeit fraud will remain an issue, and also gets further refined in its technique, potentially with the goal of successful and effective shimming or contactless skimming. Meanwhile in the POS space, low-tech fraud like lost and stolen, sometimes combined with forms of social engineering, is also going strong, and now represents a high fraud cost for card issuers in some EU countries. Unauthorised CNP fraud remains a huge problem and main fraud cost driver. Due to criminals engaging in high tech activities like APTs and other breaches where card credentials are stored, there is no shortage of stolen credentials for sale at online marketplaces. However, with high-end preventive methods and regulations like PSD2 [1] and the RTS [2] with its requirement for SCA, criminals are changing their approach towards instead utilising various phishing and social engineering techniques to perform fully authenticated CNP transactions, either themselves or scam the victims to unknowingly perform them. It is also key that the security of new products, e.g. mobile wallets, is being designed with that in mind.

For SEPA Credit Transfer and Direct Debit transactions, the criminals' use of impersonation and deception scams, as well as online attacks to compromise data, continued to be an important factor behind fraud losses related to these types of payments. In all these methods, criminals target personal and financial details which are used to facilitate fraudulent transactions. More in particular during the past year an increase was noted in Authorised Push Payment fraud (see Section 3.3).

An important aspect to mitigate the risks and reduce the fraud related to payments is the sharing of fraud intelligence and information on incidents amongst PSPs. However, often this is being limited by rules and regulations related to data protection, even more so in the case of cross-border sharing. In this context, it should be noted that the European Commission proposal for a regulation on payment services ("PSR") published in June 2023 includes provisions on data sharing for fraud prevention.

It is also worthwhile mentioning that the EPC, upon proposal from its Payment Scheme Fraud Prevention Working Group (PSFPWG), has launched in April 2022 a SEPA-wide platform for fraud information sharing between SEPA payment scheme participants. The aim is to contribute to operational payment fraud prevention by facilitating SEPA payment scheme fraud data collection and analysis, information sharing and prevention measures.

Finally, PSPs must understand the emerging threats, the possible impacts and should keep investing in appropriate security and monitoring technologies as well as in customer awareness campaigns while society should cater for early education on security and social engineering risks.

Social Engineering: Final Considerations/Conclusions

Social engineering remains an important attack factor which is further increasing – notably in relation to APP fraud.

- Business email compromise and phishing emails are forms of social engineering that have been particularly developed
- It is often used as an enabler for other types of attacks and is applied in the mobile world as well.
- Appropriate education about social engineering remains a crucial factor to combat both phishing and APP scams.
- Technical measures such as securing the email platforms and blocking the phishing websites are also important in combating social engineering.

Malware: Final Considerations/Conclusions

Malware is a major threat that can cause significant damage on both companies and individuals. All stakeholders involved in payment processes should take appropriate mitigation measures.

- Consumers should make sure that their devices, including mobile devices, are always well protected and they should follow the awareness campaigns provided by the authorities and the PSPs on this matter.
- Customer relations departments of PSPs should well inform their customers on maintaining their devices up to date with security software to reduce the malware related risk.
- Service providers or PSPs internal IT departments should implement necessary technical measures protecting their platforms against this type of attacks.
- If cloud services are used, the PSPs must identify and evaluate the relevant assets, define the appropriate security controls, evaluate and choose the cloud providers on the basis of international standards for governance and security.

APT: Final Considerations/Conclusions

One of the most lucrative payment fraud forms now and for the future seems to be APT. APTs have become a significant challenge for many cybersecurity professionals around the world.

It must be considered as a potential high risk for the payment infrastructure and for all network related ecosystems.

With a minimal of criminals involved, a maximum result can be established. Therefore, all users will need to consider utilizing new defence mechanisms in order to protect their data.

A mixed approach made of traditional tools, new advanced behaviour-based detection solutions with improved automated monitoring, correlation and analysis, and improved incident response capabilities can aid system security administrators in identifying these hard-to-detect intrusions.

DdoS: Final Considerations/Conclusions

DDoS attacks have been an increasing threat in the past few years, given the fact that the number of infected end points available and the size of attack are increasing. The expected future, and already seen in some countries, is that more sophisticated combined attacks will take place.

A further development could be that a successful DDoS attack could distract the PSP's attention from fraudulent transactions, leading to more "successes" for criminals with phishing and/or malware attacks on Internet banking.

The probability of these attacks continuing in the near future is high (e.g., in view of the increased usage of IoT devices) and financial and payments sector organisations remain potential targets.

Measures to mitigate the basic kind of DDoS attack should be common – and seem to be common – to all financial institutions.

Furthermore, it should be evaluated whether the current security architecture and countermeasures are still sufficient.

Collaboration is critical for effective DdoS mitigation and making the financial sector more resilient. On a national level this would mean that PSPs, universities, internet service providers, internet exchanges, responsible governmental cyber authorities, and the national central bank need to work together. To reduce the number of DdoS attacks the (national) police force has to be

involved as well by exchanging information, collecting evidence, intervening in payments to DdoS-as-a-service suppliers and so on.

Botnets: Final Considerations/Conclusions

As a result of the evolutions that botnets made, they have been very successful in 2020, and will probably continue so in the following years. The growth of the IoT ecosystem and with no end in sight for the relaxed security they inherently have, will be a fruitful area for exploit.

In respect to payment threats the use of botnets for DdoS will continue to be a relevant threat but keeping in mind that financial gain for the attackers is mainly obtained through extortion or similar techniques. It seems that botnet DdoS may achieve more advantageous gains extorting other time dependent activities (e.g. events) or through other extortion-based attacks (e.g. ransomware).

Account verification attacks and payment credential compromise, at the European level, will be mitigated by the adoption of Strong Customer Authentication as required under PSD2 [1]. Compromising knowledge factors on a compromised system has historically been a reasonably achievable task for malware. Compromising two factors of different natures and usage of dynamic linking will elevate the bar for the attacker to be successful.

It is foreseeable that botnets will tend to be potentiated for other malicious activity not directly related to payments, given the recently increased measures through PSD2 compliance.

- The measures to combat botnet threats and the effects of related attacks are applicable to infrastructures, software development and IoT devices covering both home and small business and enterprise systems installation.

Third-party compromise, supply chain attacks and outages: Final Considerations/Conclusions

Supply chain attacks could potentially have a severe impact. It should therefore be considered as a potential high risk that PSPs should mitigate. DORA provides fundamental principles that guide the management, by financial entities, of IT risks deriving from third parties:

- Map all ICT systems, including third-party service providers.
- Define a third-party management framework.
- Set specific requirements for outsourcing of ICT systems and services.

As best practice, PSPs should conduct a risk assessment process to identify dependencies on third-party providers. This should include critical IT supplier dependencies, customer dependencies, the mapping of critical software and single point of failure.

Monetisation Channels: Final Considerations/Conclusions

Payment fraud often leverage monetisation channels such as: cash withdrawal, no traceable purchase, money transfer, transactions with anonymous virtual currencies.

PSPs should take appropriate measures against money-mule related fraud, such as:

- Raise Awareness among target groups of customers that can involuntarily become mule.
- Register/ share identified mules by monitoring suspect accounts or bank changes of customers who potentially can become mules, to detect this behaviour at a very early stage.
- Regulators and PSPs should consider having mechanisms in place to react and stop supporting service practices or to put related transactions on hold, until further investigated, if transaction patterns indicate potential ”mule activity”.

- Develop mechanisms and analysis to detect complex mule and money laundering schemes, on a cooperative and cross-border basis.

Annex I – Summary Threats versus Controls and Mitigations

Social Engineering Section 3.1.1	Awareness campaigns for consumers, SMEs and corporates, and for PSPs staff Technical measures for email security (SPF, DKIM, DMARC) Use of authentication mechanisms that do not expose user credentials Transaction filtering and monitoring Takedown of phishing web sites
	Applicable to the following payment-relevant processes: On-boarding/provisioning, Request-to-Pay/Invoicing, Initiation/Authentication, Execution
Malware Section 3.1.2	Regular software updates on consumer devices including mobile devices Firewalls and antivirus on consumer devices Information campaigns by PSPs customer relations departments, including awareness about danger of opening attachments Script and macro blockers, IPS / IDS functionality Limited usage of admin rights Web traffic and email content analysis Specific controls and mitigation measures targeting Cloud services
	Applicable to the following payment-relevant processes: On-boarding/provisioning, Request-to-Pay/Invoicing, Initiation/Authentication, Execution
Advanced Persistent Threats Section 3.1.3	Behaviour analysis tools Real time advanced security data analytics Incorporation of security threat intelligence into infrastructure Advanced IP scanner/ APT scanner Red Team/Blue Team approach Five styles of Advanced Threat Defense Framework
	Applicable to the following payment-relevant processes: Execution

Distributed Denial of Service Section 3.1.4	Dynamic DDoS security control framework DDoS mitigation scrubbing service Periodic tests of anti DDoS measures Security intelligence feeds and incident response team "Forensic ready" logging
	Applicable to the following payment-relevant processes: Execution
Botnets Section 3.1.5	Blacklisting Sinkholing and blocking Distribution of fake/traceable credentials DNS-based countermeasures Direct takedown of C&C server Packet filtering on network and application level Walled gardens Peer-to-peer countermeasures Infiltration and remote disinfection Take downs by law enforcement Awareness raising and co-operation
	Applicable to the following payment-relevant processes: Execution
Third-party and supply chain attacks Section 3.1.6	Management of relations with suppliers in a way to ensure effectiveness of the contractual clauses related to IT security measures. Apply a risks assessment process able to identify dependencies on third-party suppliers.
Monetisation Channels Section 3.1.7	Raise awareness Register/ share information about identified mules Monitor, detect and stop mule-like behaviour at PSP and regulator level Detect complex mule and money laundering schemes
Liability for social engineering fraud Section 3.1.8	Involved stakeholders should be aware of ongoing discussions

Table 6 Summary threats versus controls and mitigations