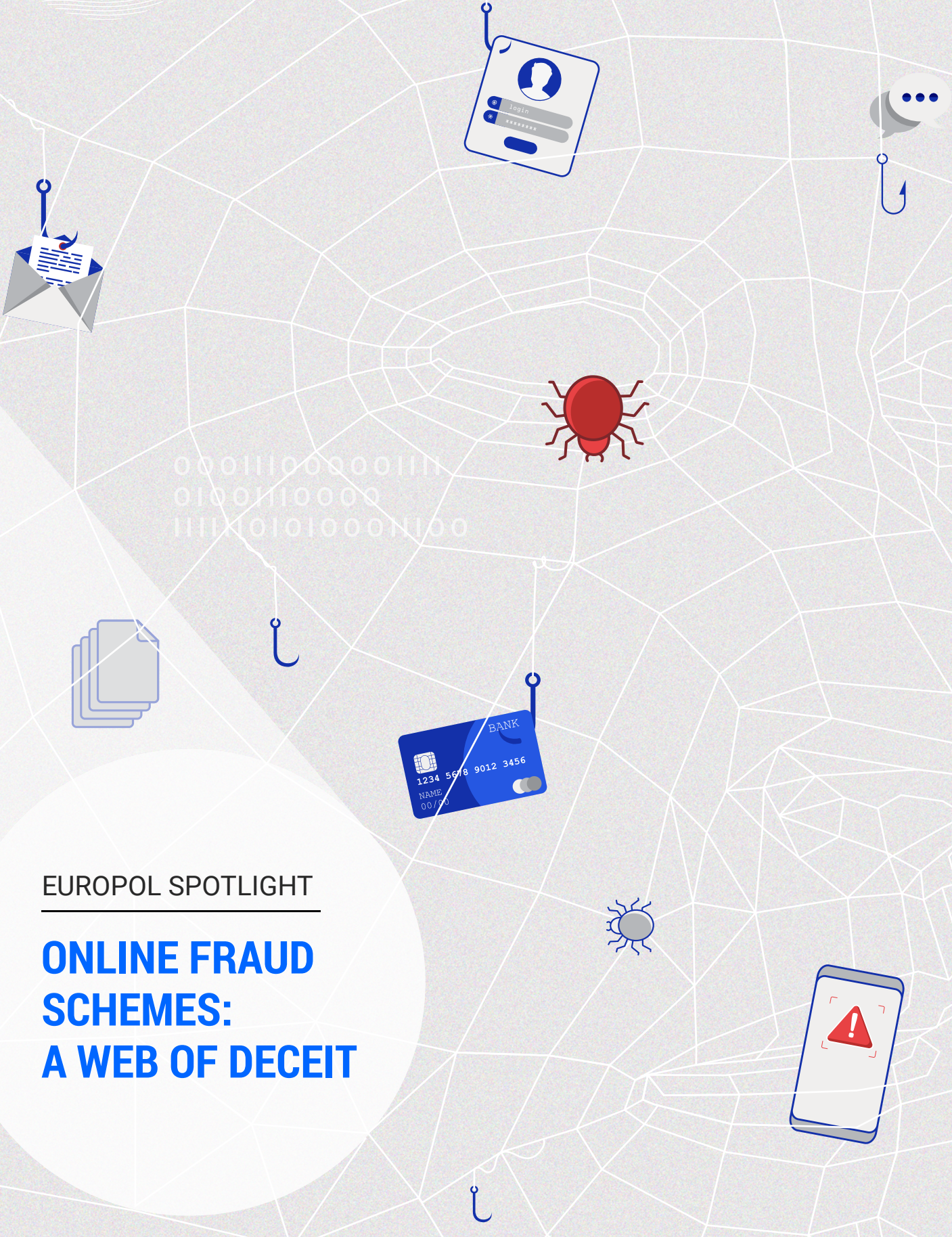
EUROPOL

IOCTA



EUROPOL SPOTLIGHT

ONLINE FRAUD SCHEMES: A WEB OF DECEIT

Contents

Key terms

ACCOUNT CHECKER: a software tool that verifies the validity of login credentials – such as usernames and passwords – for a particular service or platform. In online fraud schemes (OFSs), an account checker is a bot that takes lists of leaked or stolen credentials (e.g. usernames and passwords) and tests them against websites to access accounts.

BOT: automated software that is programmed to perform repetitive tasks.

CARDING: fraudulent use of stolen credit card data. Sometimes called credit card stuffing or card verification, it involves a series of multiple attacks usually performed by bots (software used to perform automated operations) to identify which card numbers or details can be used to make purchases. Thanks to the bots, criminals are able to make parallel automated operations to attempt purchase authorisation.

CRACKING TOOL: software deployed to break through security measures on systems and applications.

DEEPFAKE: technology that uses artificial intelligence (AI) software to make synthetic duplicates of real people's voices, images and videos. In OFSs, deepfake is an impersonation technique.

MALWARE: software that is designed to infiltrate computer systems or mobile devices without the owner's consent to gain control over the device, steal valuable information or corrupt data. The word is a portmanteau of 'malicious' and 'software'.

MAN-IN-THE-MIDDLE (MITM) ATTACK: the attacker places himself between two communicating parties and relays messages for them, while the parties believe they are communicating with each other directly and securely.

ONE-TIME PASSWORD (OTP): a password that is valid for only one login session or transaction on a computer system or other digital device. The OTP is usually sent by banking institutions to customers to authorise a money transfer. Also known as a one-time PIN, one-time authorisation code or dynamic password.

PHISHING: a form of social engineering, characterised by unsolicited communications which appear to come from a reputable source (often impersonating a bank institution, delivery company or judicial authority). Generally, these communications solicit payments or contain malicious links that land on fraudulent websites (either a domain created by the criminals or a compromised legitimate website). They may also contain attachments that will install malware if opened.

SMISHING: a form of phishing using text messages or common messaging apps.

SOCIAL ENGINEERING: the main technique used in OFSs. Social engineering means the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. It can take many forms, but always relies on psychological manipulation and emotional attacks.

THIRD-PARTY SHOPPING SOFTWARE: any software developed outside of the vendor's website or the vendor's main website provider.

VISHING: a form of phishing using voice calls and voicemails.

Key findings

Online fraud schemes represent a major crime threat in the EU and beyond as online fraudsters generate multiple billions in illicit profits every year to the detriment of individuals, companies and public institutions.

Criminal networks involved in online fraud schemes are persistent and driven by opportunism. Their chain of crime is business-like, facilitated by the growing presence of accessible enablers and the wide availability of crime-as-a-service.

Fraudsters display sophisticated modi operandi, which are usually a combination of different types of fraud. Victims of fraud are often re-victimised within the same criminal scheme.

Social engineering techniques that fraudsters use have been growing in complexity. Criminals adapt these techniques according to the profile of the victim and the typology of fraud.

Investment fraud and business e-mail compromise (BEC) fraud remain the most prolific online fraud schemes. Criminal networks involved in these schemes pose a high threat, given their level of organisation and resilience.

Charity scams leveraging emergency situations have increased. This was visible during the COVID-19 pandemic, the Russian invasion of Ukraine and the earthquake in Türkiye and Syria. Fraudsters show great versatility in modelling their narratives around current crises.

While physical skimming is an ever-diminishing threat in the EU, relay attacks targeting payment card chips (shimming) are increasingly being detected.

Logical attacks on ATMs still occur in the EU, with criminal networks testing ways to exploit new vulnerabilities at the ATMs they target.

Digital skimming is a persistent threat that results in the theft, re-sale and misuse of credit card data. A major evolution in digital skimming is the shift from the use of front-end malware to back-end malware, making it more difficult to detect.

Introduction

Online fraud schemes (OFSs) comprise a wide range of criminal activities that are exclusively or primarily perpetrated online or with the use of computers; we call this cyber-enabled. The increasing online presence of individuals, businesses and institutions has prompted many fraud schemes to shift from the physical world to the digital environment. Although online fraud specifically occurs online, such schemes can comprise both online and offline operations.

A fraud scheme is perpetrated with the intention of defrauding victims of their assets using false and deceitful pretexts, or with the use of cyber-attack techniques. This results in the voluntary or involuntary transfer of personal or business information, money or goods to criminals.

Today, OFSs represent a major crime threat in the EU and beyond, with criminals generating multi-billion illicit profits by targeting individuals, private companies and public institutions. Some types of OFS specifically target banking systems. OFSs are carried out by opportunistic individuals and by highly organised criminal networks.

Fraudsters exploit digital tools that have been produced and marketed by lawful businesses and service providers and also create their own illegal tools or buy others manufactured by cybercriminals. To identify their victims and communicate with them, fraudsters make extensive use of legitimate websites, email service providers, dating apps, social media and instant messaging services, as well as traditional telephone and voice over IP (VoIP) services.

Virtual private networks (VPNs) are commonly used to conceal offenders' IP locations. Remote Administration Tools (RATs) provide scammers access to victims' computers from a distance and let them install malicious software, change settings, run applications and access all the victims' data, including two-factor authentication (2FA) details.

Fraud is the most frequently identified predicate offence that involves the misuse of cryptocurrencies. Online fraudsters commonly misuse digital currencies, crypto-wallets and crypto-exchange platforms. This misuse includes the depositing, transferring and laundering of fraud proceeds as well as perpetrating cryptocurrency investment fraud.

Criminals misuse bank accounts, digital wallets, instant money transfer and peer-to-peer services to obtain money transfers from their victims and transfer these sums across country borders and jurisdictions. Additionally, fraudsters create fake websites, fake ads on legitimate websites and landing pages, and fake online trading platforms, not forgetting bots, chatbots, computer malware, mobile malware and phishing kits.

A fast-growing threat

OFSs are a flourishing criminal market. Online fraudsters target millions of victims across the EU every day, and the impact of these crimes is enormous and increasing. Not only are there the direct financial losses for the victims (with some instances of fraud amounting to millions of euros in damages), but also the costs of investigation by law enforcement and recovery and reimbursement by financial service providers.

Compared to past scenarios where fraud schemes were perpetrated chiefly in person, modern fraudsters exploit the increasing online presence of citizens, businesses and public institutions to skilfully target the vulnerabilities of each segment of society. The harm from online fraud is exacerbated by the detrimental effect on the victims' mental and physical health and the common re-victimisation.

Fraudsters are capable of adapting their modi operandi to emerging trends and socio-economic developments, quickly integrating innovative technologies and tools into their business models. These criminals are often non-EU nationals operating from abroad. Similarly, stolen funds are swiftly transferred out of the EU, bringing further challenges to investigations, asset tracing and recovery.

Online fraud against individuals and the private and public sectors

Investment and business e-mail compromise (BEC) fraud remain the most prolific forms of OFS. Phishing campaigns also persist, adding new narratives to lure victims into transferring money to the offenders. Fraudsters continue to show high levels of adaptability, leveraging crises such as the

Russian war of aggression against Ukraine or the earthquake in Türkiye and Syria, to scam their victims.

There are other typologies of fraud that continue to have a strong impact on victims. Tech-support scams cause huge losses by tricking the victims into providing access to their computer systems to obtain login credentials and credit card data. Romance fraud is widely reported in the EU, sometimes in combination with other fraud schemes targeting the same victims.

Reticence in reporting online fraud to law enforcement is very common, often due to a sense of shame individuals feel or a company's fear of reputational damage. This result is an under-reporting of the phenomenon. Fraud victims are often re-victimised by different types of fraud within the same criminal process; victims' information is monetised to its full extent and frequently sold on to criminals, leading targets of fraud to be re-victimised.

Criminal networks are increasingly resorting to social engineering[1]. This technique uses deception to manipulate individuals into voluntarily or involuntarily divulging confidential or personal information to fraudsters. As authentication mechanisms have been strengthened with the introduction of 2FA measures such as one-time passwords and digital fingerprints, criminal networks not only seek out credit card details, but also access accounts through account takeover (ATO)[2].

Phishing is a key access vector for most types of fraud, aiming to intrude into systems, steal data or extort money. This technique may also involve installing malware to steal credentials and/or banking information[3]. Phishing can also take different guises, depending on the means of communication in use. Common alternative techniques are smishing (SMS phishing) and vishing (voice phishing).

1 Europol, 2020, Internet Organised Crime Threat Assessment (IOCTA), available at https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

2 Directive (EU) 2015/2366 (payment service directive 2 – PSD 2) provides the legal foundation for the further development of a better integrated internal market for electronic payments within the European Union (EU). It establishes comprehensive rules for payment services, with the goal of ensuring harmonised rules for the provision of payment services in the EU and a high level of consumer protection. The directive requires Secure Customer Authentication (SCA) for most electronic payments, involving two-factor authentication (2FA) or multi factor authentication (MFA) to access services and/or authorise transactions. Full Directive available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

3 Europol, 2023, Cyber-attacks: The apex of crime-as-a-service, Europol Spotlight, IOCTA 2023, available at https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023

Impersonation is a technique used in the majority of online fraud schemes to deceive victims. Spoofing is one example of a very effective technique to gain victims' trust, whereby fraudsters make a phone call or send a text message that bears a different caller ID than that of the telephone from which the call was actually placed. Some criminal networks provide spoofing-as-a-service to other fraudsters[4].

Investment fraud

Investment fraud persists as a key threat in the EU, targeting thousands of victims and generating millions in illicit profits every year. Criminal networks involved in this type of fraud show great levels of adaptability by constantly refining and improving their modi operandi and leveraging new investment products that are highly in demand.

Fraudsters commonly seek out victims on social media platforms, but also use e-mail, instant messaging applications or dedicated websites with ads enticing victims to open online trading portfolios and lure them in with initial benefits. Once the victim starts asking for clarification on the investment returns or becomes suspicious, the criminals pretend that there are legitimate reasons why they cannot withdraw their money, such as fees or state taxes. The victim is then asked to pay more money to release their funds. In order to provide the victim with a sense of legitimacy, criminal networks involved in investment fraud make extensive use of call centres. These call centres operate in different languages and the operators are in some cases unaware of the criminal activities behind the work they do.

Some investment fraud criminal networks use tactics such as pyramid schemes, namely encouraging victims to recruit other victims. This process provides fraudsters with a wider victim base and effortlessly increases their criminal profits.

A concerning threat around investment fraud is its use in combination with other fraud schemes against the same victims. Investment fraud is sometimes linked to romance scams: criminals slowly build a relationship of trust with the victim and then convince them to invest their savings on fraudulent cryptocurrency trading platforms, leading to large financial losses. Following the theft of the investments and the fraud being

4 Europol, 2022, Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests, available at https://www.europol.europa.eu/media-press/newsroom/news/action-against-criminal-website-offered-%E2%80%98spoofing%E2%80%99-services-to-fraudsters-142-arrests

uncovered, criminals often contact their victims posing as lawyers or law enforcement agents offering help to retrieve their funds in exchange for a fee. The actual perpetrators of such schemes are sometimes victims of forced labour themselves.

Fraudsters advertise a wide range of investment products (such as stocks, binary options and pension funds) and adapt to socio-economic trends by continuously shifting their focus to attractive products. The most reported investment fraud products in the EU are cryptocurrencies. This type of fraud has shown to be extremely profitable, rising in parallel with the price surge on common cryptocurrencies[5] and the proliferation of new ones. However, the cryptocurrencies market saw a sharp drop in 2022 with a strong decrease in cryptocurrency prices[6] leading to a decline in the revenue from the crypto scams detected in 2022[7]. Though this could be related to a general market decline, under-reporting might also play a role, particularly in relation to crypto-investment fraud combined with romance scams[8].

Business e-mail compromise (BEC)

BEC is a form of digitally-enabled fraud perpetrated against private companies with the use of social engineering techniques. The most common types of BEC are **chief executive officer (CEO) fraud** (where criminals make urgent payment requests by impersonating a company executive) and **fake invoice fraud** (which involves fraudsters impersonating business partners and requesting payment on fictitious invoices, or exploiting genuine invoices where the legitimate suppliers' bank details have been altered).

To perpetrate their scheme, fraudsters illicitly gain access to a company's e-mail communication, gaining insights into internal structures and operating procedures. In some cases, fraudsters use phishing techniques to obtain personal data, which they then use to intercept and manipulate corporate communication.

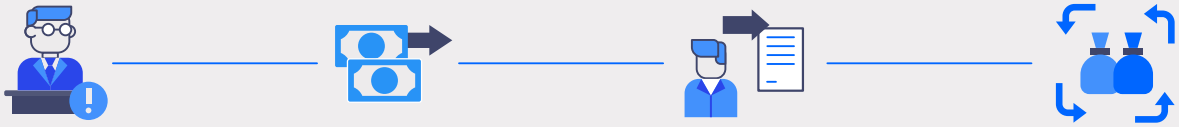
5 Chainalysis, 2022, Crypto Crime Report 2022, available at https://go.chainalysis.com/2022-Crypto-Crime-Report.html

6 J. Yang, J. Gunzberg, M. Good, B. Keoun, CoinDesk, 20 December 2022, CoinDesk Market Outlook: 4Q Crypto Gloom Spills Into 2023, available at https://www.coindesk.com/consensus-magazine/2022/12/20/2023-crypto-price-market-outlook/

7 Chainalysis, 2023, Crypto Crime Report 2023, available at https://go.chainalysis.com/2023-crypto-crime-report.html

8 Ibid.

CEO FRAUD



STEP 1

A fraudster contacts an employee in the finance department at a company, posing as a high-ranking executive (CEO or CFO).

STEP 2

The fraudster requests an urgent transfer of funds and absolute confidentiality, invoking a sensitive situation (e.g. a tax inspection, merger or acquisition)

STEP 3

The fraudster pressures the employee into not following the regular authorisation procedures. Instructions on how to proceed are given by a third person or via e-mail (optional).

STEP 4

The employee transfers funds to an account the fraudster controls. The money is then transferred to accounts across multiple jurisdictions.

BEC, and particularly CEO fraud, have grown in sophistication, focusing on upper-level management. Victims sometimes conclude several transfers before realising the scam, while the ill-gotten gains are quickly split through accounts based in multiple countries and laundered.

Criminal network involved in CEO fraud

In 2021, a Franco-Israeli criminal network was involved in large-scale CEO fraud targeting companies located in France. The perpetrators used the identities of the company's CEOs and trusted business partners (such as lawyers working for accounting companies or consultants) to request large, urgent and confidential transfers. One of the companies targeted lost almost EUR 38 million in just a few days. The suspects laundered the criminal proceeds through a pre-existing money laundering scheme involving multiple bank accounts in the EU, China and Israel[9].

An indicator of the growing sophistication of CEO fraud is the use of deepfakes. In one case, criminals used deepfake audio to impersonate the CEO of a company and elicit the transfer of the equivalent of EUR 35 million[10].

9 Europol, 2023, Franco-Israeli gang behind EUR 38 million CEO fraud busted, available at https://www.europol.europa.eu/media-press/newsroom/news/franco-israeli-gang-behind-eur-38-million-ceo-fraud-busted

10 Europol, 2022, Facing reality? Law enforcement and the challenge of deepfakes, Europol Innovation Lab observatory report, available at https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes

Phishing campaigns

Massive phishing campaigns based on various themes continue to target millions of victims in the EU, causing significant financial losses and reputational damage to the entities they impersonate. Phishing campaigns are perpetrated mostly via email, but also via SMS, and often entail money transfer requests and impersonation of well-known businesses or government entities.

Victims receive false information about overpayments, tax requests, announcements of detected crimes, or promises of significant cash prizes, goods or services. Fraudsters find or purchase contact lists and e-mail addresses online. The increased availability of phishing kits sold online allows more criminal networks to be successful in their phishing attacks, regardless of the level of organisation and technical expertise.

Police-themed scams

In an online scam in 2022, fake correspondence was sent via email and social media, purportedly from Europol departments and senior staff. The message told victims that they had visited websites hosting child sexual abuse material and urged them to reply to an email address. Respondents were asked to make a payment of between EUR 3 000 and 7 000 via bank transfer or instant money services to avoid prosecution[11].

Fraudsters are always driven by opportunism, luring their targets with attractive claims. Recurring narratives used for phishing campaigns relate to ongoing crises to exploit people's emotional involvement. Charity scams are a particularly unscrupulous type of phishing campaign, profiteering from an individual's generosity towards those in need. Criminals pose as genuine organisations to obtain donations, victimising both the donor and the legitimate aid agency. Scams exploiting crises have been detected increasingly in the last few years, first in relation to the COVID-19 pandemic, and more recently in the context of the Russian invasion of Ukraine and the earthquake in Türkiye and Syria.

11 Europol, 2021, Beware of scams involving fake correspondence from Europol, available at https://www.europol.europa.eu/media-press/newsroom/news/beware-of-scams-involving-fake-correspondence-europol

Leveraging the Russian war of aggression against Ukraine

Charity scams through phishing campaigns have been detected in relation to the Russian war of aggression against Ukraine. Fraudsters targeted victims across the EU under the guise of supporting Ukraine or Ukrainians. The scammers created fake webpages to solicit money using URLs that included misleading keywords. They also used fraudulent addresses to send fake emails pretending to raise funds for humanitarian efforts. In some cases, fraudsters impersonated celebrities that were heading or supporting real campaigns, or spoofed humanitarian organisations' domains, inviting victims to donate in cryptocurrency.

Online fraud against payment systems

A range of online fraud schemes are perpetrated specifically against payment systems. These specialised types of fraud use common intrusion techniques[12] to access and manipulate payment and financial systems while remaining undetected. They target the systems without the users being directly involved. The purpose is to either to steal funds or obtain personal information that is then further exploited by the criminals. This type of fraud not only has a significant financial impact on payment service providers but also causes reputational damage to legitimate vendors and undermines consumer trust.

Compromising payment systems does not directly affect users who do not experience any anomalies in their transactions. However, individuals may be a secondary target of these types of fraud. Fraud against payment systems is often followed by the theft of personal information that can then be used for further criminal acts. This could include identity theft, fraudulent financial transactions, or for refining social engineering methods to re-victimise the same individuals whose information was stolen during the first fraud scheme.

12 Europol, 2023, Cyber-attacks: The apex of crime-as-a-service, Europol Spotlight, IOCTA 2023, available at https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023

Logical attacks on ATMs

Automated teller machine (ATM) logical attacks involve electronically compromising ATMs to withdraw cash without using a bank card. These attacks continue to be an attractive avenue for criminals who exploit vulnerabilities in ATMs. ATM logical attacks comprise a coordinated set of actions aimed at gaining access to the ATM computer system, manipulating or extracting data, and controlling the dispensing function. The most common type of ATM logical attack is the **Black Box (or jackpotting) attack**. This is carried out either by connecting an unauthorised external device to the ATM or by injecting malware into it. In both instances, the aim is to send commands directly to the ATM cash dispenser so that it ejects cash.

Skimming

Digital skimming is a common technique that allows fraudsters to steal credit card credentials from online vendors' checkout pages or credentials that are stored online (often in mobile apps). Digital skimmers steal payment data from input fields on existing payment forms or redirect unsuspecting users to fake checkout pages. Compromised card details are sold on dedicated websites and dark web marketplaces (also known as card dumps). These illicitly obtained credentials are often used for carding, usually performed by bots that test the validity of stolen card data, and to make purchases. Through the bots, criminals are able to perform simultaneous automated operations to attempt purchase authorisation.

Magecart

Magecart is a well-known digital skimming technique, named after the most known cybercrime group that specialises in cyber-attacks involving digital credit card theft by skimming online payment forms. Its name comes from Magento, the first type of third-party shopping software targeted back in 2015. Since then, digital skimming attacks have grown in scope, scale, impact and sophistication. Thousands of online stores around the world have been infected[13], resulting in their customers' personal data being collected at check out.

13 As of April 2023, Sansec has identified over 70 000 e-commerce websites that have suffered a Magecart attack. Available at https://sansec.io/docs/what-is-magecart

Physical skimming on bank and credit cards is diminishing in the EU, however it remains a threat outside its borders. Physical skimming captures data from the magnetic stripe on cards. It is now forbidden to use the magnetic strip for transactions within the EU in compliance with the new Strong Customer Authentication (SCA) requirement of the revised Payment Services EU Directive (PSD2)[14]. This Directive seeks to add extra layers of security to electronic payments. The magnetic stripe will not be required on newly issued payment cards in many regions from 2024[15]. Nevertheless, EU criminal networks with expertise in this crime area may shift their attention to countries where there is still widespread use of the magnetic stripes.

Shimming

Similar to skimming, shimming is an interception and/or a manipulation of information flowing between a card and the chip interface of a card reader. In recent years, relay attacks targeting payment card chips have been increasingly reported in the EU. In a relay attack, an attacker intercepts communication between two parties and then relays it to another device. The attacker does not need to initiate any communication between sender and receiver, as is the case a Man-in-the-Middle attack.

Account takeover (ATO)

Recent investigations into the trade in compromised credentials show the growing threat of the illicit trade in personal data. The extensive compromised credentials market and readily available illicit tools are making fraudsters less dependent on specific expertise, as some tasks within OFSs can be easily outsourced.

Account takeover is a form of hacking that occurs when criminals illegally access a victim's online account for their own gain. Targeted accounts (such as online banking, email accounts or social media profiles) are valuable to criminals as they can hold funds and access specific services or relevant private information that can then be sold online. ATO is now considered

14 PSD2 is the acronym for the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366. The Second Customer Authentication (SCA) measure WAS introduced in September 2019 following the entry into force of PSD2.

15 Emerchantpay, 24 May 2022, 'Mastercard is phasing out magnetic stripes', available at https://www.emerchantpay.com/insights/mastercard-is-phasing-out-magnetic-stripes/

quite an easy hacking technique to implement as cracking tools and account checkers are sold on cybercrime forums for a very low price.

The theft of digital fingerprint data from compromised devices has emerged following the introduction of digital fingerprinting as an authentication mechanism[16]. This highlights the adaptability of criminals in countering online anti-fraud systems, which is set to continue in the future.

Tokenised credit cards have become a popular means of payment. They are obtained after card tokenisation, the process of de-identifying sensitive cardholder data by converting it to a string of randomly generated numbers called token. Tokenisation protects the cardholder in the event of a data breach or other exposure. Tokenised credit cards are usually found on mobile payment services and digital wallets and can be linked to subscriptions to online services as well as to card-not-present (CNP) online purchases. Fraudsters apply several techniques to obtain the one time password (OTP) – sent by banking institutions to customers to authorise a money transfer – connected to tokenised credit cards. They can then connect the stolen credit card data to existing mobile payment systems to purchase items or obtain cash from the counter (in the countries where this is allowed).

SIM swapping is another ATO technique entailing fraudsters taking control of the victim's mobile phone SIM card (or obtaining a duplicate of the SIM card). Fraudsters deceive mobile phone operators into porting the victim's mobile number to a SIM in their possession so they can receive incoming calls and text messages and have access to sensitive data. SIM swapping is often used to obtain the OTP to authorise money transfers. In 2022, cases of SIM swapping had decreased, probably due to telecommunication providers implementing better prevention and customer identification mechanisms[17].

16 Information provided to Europol

17 Information provided to Europol

Criminal actors involved in online fraud

The criminal actors engaged in OFSs span from lone criminals to highly organised networks composed of tens, hundreds and even thousands of facilitators. Criminals are facilitated by the growing presence of enablers, such as guidelines and tutorials on fraud methods on dark web forums, phishing kits, remote administration tools, card dumps, and databases of personal data. The wide availability of crime-as-a-service has made this criminal activity more accessible.

The degree of internal organisation of such criminal networks varies according to the complexity of the fraud scheme, the geographical extent of the operations, and the intricacy of the money laundering processes. The structure of these criminal networks is typically pyramidal. Some of them resemble international corporate structures with a high level of internal organisation and sophisticated HR and they operate across multiple jurisdictions.

Criminal networks involved in OFSs accrue their profits in both fiat and cryptocurrencies. Funds are usually laundered very quickly after the fraud has taken place; by the time the victim realises the scam, the money is already split across accounts based in multiple countries and laundered. Online fraudsters make frequent use of gambling platforms to launder profits. Criminals make use of money mules to launder illicit profits and to swiftly move funds across a network of accounts, often in different countries. While money mules are sometimes recruited in criminal forums, social media remains a key recruitment environment. Sometimes, the victims of frauds are unwittingly used as money mules themselves.

The future of OFSs

Online fraud schemes are set to further expand in the future in terms of both harm and reach. New foci, new narratives, new products and new modi operandi will lure in more victims than ever. Investment fraud involving emerging products and growing economic sectors are likely to evolve too.

Online fraudsters and cybercriminals will continue to embrace new technologies and maximise their potential for harm with sensitive data as a core target. The growth of new technologies such as ChatGPT and other generative artificial intelligence (AI) variants of large language models (LLMs) will open them up to misuse, adding complexity to the existing threat. Against a backdrop of the rising trend in generative AI models, unethical variants of ChatGPT – such as WormGPT and FraudGPT – are set to evolve.

Defence from the harm of deepfakes will become an utmost necessity in the fight against online fraudsters. The metaverse may also open up new opportunities to different fraudulent schemes. Through the increasing use of innovative technologies and tools, the crime-as-a-service ecosystem will likely expand to service a wider criminal base, bringing criminal activities within the reach of more players and act as a multiplier for organised crime. Both criminal networks and lone actors will gain new and more harmful means of victimising their targets.

The state-of-the-art encryption that is used today to protect sensitive information will be challenged by the expected capability of quantum computers. Encrypted data collected today may become available to criminals in the not-too-distant future. This may facilitate a variety of criminal activities, including more threats related to social engineering and advanced phishing techniques[18].

Europol's response in the fight against online fraud schemes

Online fraud schemes are expected to further increase as a criminal threat affecting the EU, its citizens and its economy. Cybercriminals are likely to further embrace new technologies and maximise the reach of their services. The crime-as-a-service business model will likely expand to service a wider criminal base. Personal data, such as access credentials, are set to remain an extremely valuable commodity for online fraudsters.

18 Europol, 'The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement', Europol Innovation Lab observatory report, available at https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement

Europol's mission is to support EU Member States and cooperation partners in preventing and combating all forms of serious international and organised crime, cybercrime and terrorism. In 2013, Europol set up the European Cybercrime Centre (EC3) to provide dedicated support for cybercrime investigations in the EU to help protect European citizens, businesses and governments from online crime. EC3 offers operational, strategic, analytical and forensic support to Member States' investigations. EC3's dedicated Analysis Project Terminal, focused on the threat of online fraud schemes, supports international investigations and operations into fraud targeting various victims and payment systems in the EU and beyond.

IOCTA

The Internet Organised Crime Threat Assessment (IOCTA) is a strategic analysis report that provides a law enforcement-centric assessment of the latest online threats and the impact of cybercrime within the EU. It serves to inform decision-makers at strategic, policy and tactical levels in the fight against cybercrime, with a view to updating the operational focus for EU law enforcement authorities.

The IOCTA is chiefly informed by operational information shared with Europol by EU Member States and third partners, combined with expert insights and open source intelligence.

This ninth edition of the IOCTA appears in an updated format. A summary presents the main overarching findings concerning the major typologies of cybercrime, namely cyber-attacks, online fraud schemes, and online child sexual exploitation. This report, “Online fraud schemes: a web of deceit”, is the second in a series of spotlight reports covering each of these crime areas in-depth as part of the IOCTA 2023.

Your feedback matters.

By clicking on the following link or scanning the embedded QR code you can fill in a short user survey on the received strategic report. Your input will help us further improve our products.

https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. We also work with many non-EU partner states and international organisations. From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer.

EUROPOL SPOTLIGHT - ONLINE FRAUD SCHEMES: A WEB OF DECEIT

PDF | ISBN 978-92-95220-96-6 | ISSN 2600-2760 | DOI: 10.2813/543686 | QL-AN-23-003-EN-N

Luxembourg: Publications Office of the European Union, 2023

Cite this publication: Europol (2023), Online fraud schemes: a web of deceit,
Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu