Raad van de
Europese Unie

Brussel, 11 juli 2023
(OR. en)

11761/23

CYBER 184
DROIPEN 107
IA 180
JAI 998
MI 607
TELECOM 229

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	10 juli 2023
aan:	mevrouw Thérèse BLANCHET, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	COM(2023) 363 final
Betreft:	VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD waarin wordt beoordeeld in welke mate de lidstaten de nodige maatregelen hebben genomen om te voldoen aan Richtlijn (EU) 2019/713 betreffende de bestrijding van fraude met en vervalsing van niet-contante betaalmiddelen en ter vervanging van Kaderbesluit 2001/413/JBZ van de Raad

Hierbij gaat voor de delegaties document COM(2023) 363 final.

Bijlage: COM(2023) 363 final

EUROPESE
COMMISSIE

Brussel, 10.7.2023
COM(2023) 363 final

VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

waarin wordt beoordeeld in welke mate de lidstaten de nodige maatregelen hebben genomen om te voldoen aan Richtlijn (EU) 2019/713 betreffende de bestrijding van fraude met en vervalsing van niet-contante betaalmiddelen en ter vervanging van Kaderbesluit 2001/413/JBZ van de Raad

1. Inleiding

Fraude met en vervalsing van niet-contante betaalmiddelen, zoals creditcards en betaalkaarten, is voor de georganiseerde misdaad een bron van inkomsten waarmee andere criminele activiteiten, zoals terrorisme, drugshandel en mensenhandel, worden gefinancierd. Deze strafbare feiten veroorzaken aanzienlijke verliezen: in 2019 bedroeg de totale waarde van frauduleuze transacties met binnen de gemeenschappelijke eurobetalingsruimte (SEPA) uitgegeven kaarten 1,87 miljard EUR[1]. De overgrote meerderheid van frauduleuze transacties houdt verband met fraude zonder aanwezige betaalkaart (CNP-fraude): in 2019 was 80 % van de waarde van betaalkaartfraude het gevolg van CNP-transacties, d.w.z. betalingen via internet, post of telefoon[2]. in 2019 was CNP-fraude verantwoordelijk voor 1,5 miljard EUR aan fraudeverliezen, een stijging van 4,3 % ten opzichte van het voorgaande jaar[3].

Er is een duidelijke grensoverschrijdende dimensie: meer dan de helft van de totale waarde van fraude in 2019 had betrekking op grensoverschrijdende transacties binnen de SEPA. Geografisch gezien vertegenwoordigden binnenlandse transacties 89 % van de waarde van alle betaalkaarttransacties in 2019, maar slechts 35 % van de frauduleuze transacties. Grensoverschrijdende transacties binnen de SEPA vertegenwoordigden 9 % van de waarde van alle betaalkaarttransacties, maar 51 % van de gerapporteerde fraude[4].

Om deze criminaliteit op doeltreffende wijze te kunnen bestrijden, dienen de lidstaten gezamenlijk te bepalen welke handelingen als fraude met en vervalsing van niet-contante betaalmiddelen moeten worden beschouwd. Ook dienen zij te beschikken over geharmoniseerde sanctieniveaus en de operationele middelen om strafbare feiten te rapporteren en informatie tussen de autoriteiten uit te wisselen. Het Europees Parlement en de Raad hebben derhalve op 17 april 2019 Richtlijn (EU) 2019/713 betreffende de bestrijding van fraude met en vervalsing van niet-contante betaalmiddelen en ter vervanging van Kaderbesluit 2001/413/JBZ van de Raad[5] (hierna "de richtlijn" genoemd) vastgesteld. Dit verslag komt tegemoet aan het vereiste overeenkomstig artikel 21 van de richtlijn.

1.1. Doelstellingen en toepassingsgebied van de richtlijn

De doelstellingen van de richtlijn zijn het onderling afstemmen van de strafwetgeving van de lidstaten[6] op het gebied van fraude met en vervalsing van niet-contante betaalmiddelen en het verbeteren van de samenwerking tussen de bevoegde autoriteiten. Hiertoe worden in deze richtlijn minimumvoorschriften vastgesteld voor de definitie van strafbare feiten en sancties. De werkingssfeer van de richtlijn is breed en omvat elk "immaterieel of materieel, beveiligd apparaat of voorwerp of een immateriële of materiële, beveiligde registratie, of een combinatie daarvan, met uitzondering van wettige betaalmiddelen, waarmee de houder of

---

1 Europese Centrale Bank, zevende verslag over betaalkaartfraude, te raadplegen op: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.nl.html

2 Zie vorige voetnoot.

3 Zie voetnoot 1.

4 Zie voetnoot 1.

5 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32019L0713

6 Hierna wordt, tenzij uitdrukkelijk anders aangegeven, met "lidstaten" of "alle lidstaten" verwezen naar de lidstaten die door de richtlijn gebonden zijn, dat wil zeggen alle EU-lidstaten met uitzondering van Denemarken en Ierland, die niet aan de vaststelling van de richtlijn hebben deelgenomen, overeenkomstig respectievelijk het Protocol betreffende de positie van Denemarken dat gehecht is aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie (VWEU) en Protocol nr. 21 betreffende de positie van het Verenigd Koninkrijk en Ierland.

gebruiker, al dan niet in combinatie met een procedure of geheel van procedures, geld of monetaire waarde kan overmaken, waaronder door middel van digitale betaalmiddelen" (artikel 2, punt a)[7]). Zo valt bijvoorbeeld een mobiele betaaltoepassing met bijbehorende machtiging (bijvoorbeeld door middel van een pincode) onder deze definitie. Ook virtuele valuta vallen onder de richtlijn (artikel 2, punt d), en artikel 6).

In de richtlijn worden specifieke strafbare feiten gedefinieerd, te weten:

- frauduleus gebruik van niet-contante betaalinstrumenten (artikel 3);
- strafbare feiten in verband met het frauduleus gebruik van materiële niet-contante betaalinstrumenten (artikel 4);
- strafbare feiten in verband met het frauduleus gebruik van immateriële niet-contante betaalinstrumenten (artikel 5);
- fraude met betrekking tot informatiesystemen (artikel 6);
- onrechtmatige verstrekking van instrumenten die worden gebruikt om de genoemde strafbare feiten te plegen (artikel 7).

Daarnaast wordt in de richtlijn de **strafrechtelijke aansprakelijkheid** uitgebreid met de uitlokking door en medeplichtigheid aan het plegen of pogen te plegen van de hierboven genoemde strafbare feiten door natuurlijke personen en/of rechtspersonen (artikel 8).

In artikel 9 worden minimumniveaus voor maximale **sancties** voor de in de richtlijn genoemde strafbare feiten vastgesteld.

In de daaropvolgende artikelen worden minimale voorwaarden vastgesteld voor de **aansprakelijkheid van rechtspersonen** (artikel 10) en sancties, die al dan niet strafrechtelijke boeten omvatten, en wordt een lijst met voorbeelden van mogelijke sancties gegeven (artikel 11).

Het doel van artikel 12 is ervoor te zorgen dat de in de richtlijn genoemde daders worden vervolgd voor de strafbare feiten op grond van de artikelen 3 tot en met 8 van de richtlijn. De **rechtsmacht** van een lidstaat moet worden vastgesteld indien a) het strafbare feit geheel of gedeeltelijk op zijn grondgebied is gepleegd en/of b) de dader onderdaan is van de lidstaat. Met andere woorden, artikel 12, lid 1, punt a), van de richtlijn bevat het territorialiteitsbeginsel, terwijl punt b) betrekking heeft op het actief nationaliteitsbeginsel.

In artikel 13, lid 1, van de richtlijn is bepaald dat **opsporingsmiddelen** voor het onderzoeken en vervolgen van de in de artikelen 3 tot en met 8 bedoelde strafbare feiten doeltreffend en evenredig moeten zijn en de verantwoordelijke personen, eenheden en diensten ter beschikking moeten staan. Overeenkomstig artikel 13, lid 2, van de richtlijn moet informatie over de in de artikelen 3 tot en met 8 bedoelde strafbare feiten onverwijld ter kennis worden gebracht van de autoriteiten die die strafbare feiten opsporen of vervolgen.

Met betrekking tot de uitwisseling van informatie worden de lidstaten er in artikel 14 toe verplicht ervoor te zorgen dat zij nationale **contactpunten** beschikbaar stellen die 24 uur per dag en 7 dagen per week operationeel zijn, zodat alle dringende verzoeken uit het buitenland binnen acht uur beantwoord kunnen worden.

[7] Alle genoemde artikelen verwijzen naar de artikelen van de richtlijn, tenzij anders aangegeven.

Bovendien worden de lidstaten er in artikel 15, lid 1, van de richtlijn toe verplicht om passende kanalen op te zetten om de in de artikelen 3 tot en met 8 bedoelde **strafbare feiten onverwijld aan overheidsinstanties te melden**. In het bijzonder worden financiële instellingen aangemoedigd om vermoedelijke fraude te melden bij justitiële en rechtshandhavingsautoriteiten (artikel 15, lid 2). Het melden hiervan is vaak het startpunt van de strafrechtelijke opsporing (overweging 27).

Tot slot hebben de artikelen 16 en 17 van de richtlijn betrekking op respectievelijk **bijstand en ondersteuning aan slachtoffers** en **preventie**.

1.2 Doel en methode van het verslag

In artikel 20 van de richtlijn worden de lidstaten ertoe verplicht de nodige wettelijke en bestuursrechtelijke bepalingen in werking te doen treden om uiterlijk op 31 mei 2021 aan de richtlijn te voldoen en de Commissie daarvan in kennis te stellen.

Dit verslag komt tegemoet aan het vereiste overeenkomstig artikel 21 van de richtlijn, dat voorschrijft dat de Commissie een verslag indient bij het Europees Parlement en de Raad waarin wordt beoordeeld in welke mate de lidstaten de nodige maatregelen hebben genomen om aan de richtlijn te voldoen. Dit eerste krachtens artikel 21 uitgebrachte verslag biedt een overzicht van de belangrijkste omzettingsmaatregelen van de lidstaten.

De lidstaten hebben de richtlijn omgezet door informatie over de relevante wetgeving en administratieve maatregelen te verzamelen, die te analyseren, nieuwe wetgeving op te stellen of — in de meeste gevallen — bestaande wetgeving aan te passen, te zorgen dat deze aangenomen wordt, en ten slotte verslag erover uit te brengen aan de Commissie.

Op de datum van omzetting (21 mei 2021) hadden negen lidstaten de Commissie in kennis gesteld van de volledige afronding van de omzetting van de richtlijn en van hun omzettingsmaatregelen. In juli 2021 werden door de Commissie inbreukprocedures wegens niet-mededeling van nationale omzettingsmaatregelen ingesteld tegen de overige zestien lidstaten: AT, BE, BG, CY, CZ, EL, ES, HR, IT, LU, LV, MT, PL, PT, RO en SI[8]. Hoewel vijftien lidstaten sindsdien hun omzettingsmaatregelen hebben aangemeld, loopt er op 30 april 2023 nog steeds een inbreukprocedure wegens niet-mededeling van nationale omzettingsmaatregelen tegen BG[9].

De volgende beschrijving en analyse in dit verslag zijn gebaseerd op de informatie over nationale omzettingsmaatregelen die de lidstaten tot 31 januari 2023 hadden ingediend. Na die datum ontvangen kennisgevingen zijn buiten beschouwing gelaten. Alle aangemelde maatregelen inzake nationale wetgeving werden in aanmerking genomen, evenals rechterlijke beslissingen en, indien van toepassing, gemeenschappelijke rechtstheorie. Daarnaast heeft de Commissie tijdens de analyse in voorkomend geval rechtstreeks contact opgenomen met de lidstaten voor extra informatie of toelichting. Alle verzamelde informatie is in de analyse meegenomen.

[8] De lidstaten worden in dit document aangeduid met de in onderstaand document vermelde codes: http://publications.europa.eu/code/nl/nl-5000600.htm

[9] Informatie over de beslissingen van de Commissie inzake inbreukprocedures is te vinden op: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=nl

Naast de kwesties die in dit verslag aan de orde komen, kunnen er ook andere problemen zijn bij de omzetting en andere bepalingen die niet aan de Commissie zijn meegedeeld, of kunnen zich in de toekomst ontwikkelingen voordoen, zowel op het gebied van wetgeving als in andere domeinen. Dit verslag weerhoudt de Commissie er daarom niet van sommige bepalingen verder te evalueren en zo de lidstaten te blijven ondersteunen met de omzetting en uitvoering van de richtlijn.

2. Omzettingsmaatregelen

2.1 Wettelijke definities

Artikel 2 bevat de definities van de belangrijkste termen die in de richtlijn worden gebruikt, namelijk: niet-contant betaalinstrument; beveiligd apparaat of voorwerp of beveiligde registratie; digitaal betaalmiddel; virtuele valuta; informatiesysteem; computergegevens; rechtspersoon.

De lidstaten hebben de definities over het algemeen omgezet door zich te baseren op wetten die dateren van vóór de richtlijn of die zijn aangenomen na de inwerkingtreding ervan. Hoewel er in bepaalde gevallen geen bepalingen met specifieke definities zijn, worden de strafbare feiten omgezet door middel van algemene strafrechtelijke bepalingen die een breder toepassingsgebied hebben, bijvoorbeeld bepalingen over diefstal. Het niet melden van een letterlijke omzetting van de definitie betekent dus niet noodzakelijk dat de definitie niet volledig of niet conform is.

Bovendien verwijzen verschillende definities naar definities die zijn opgenomen in andere richtlijnen.

a) Niet-contante betaalinstrumenten

Uit de evaluatie is ten minste één geval van onvolledige omzetting naar voren gekomen, aangezien de in Kaderbesluit 2001/413/JBZ van de Raad vastgestelde definitie niet was bijgewerkt. In de definitie wordt derhalve alleen verwezen naar materiële betaalinstrumenten en niet naar "beveiligd apparaat of voorwerp of […] beveiligde registratie, of een combinatie daarvan", zoals vastgesteld in de definitie van de richtlijn.

b) Beveiligd apparaat of voorwerp of beveiligde registratie

Verscheidene lidstaten hebben deze definitie niet omgezet (BG, CZ, EE, ES, FI, HR, LT, NL, PL, PT, RO, SI). Dit wordt niet noodzakelijkerwijs beschouwd als een geval van niet-naleving, aangezien de betekenis doorgaans voor zich spreekt of kan worden afgeleid uit de formulering van de definitie van niet-contant betaalinstrument. In bepaalde landen wordt het concept uitgelegd in voorbereidende werkzaamheden.

c) Digitale betaalmiddelen en virtuele valuta

Deze twee definities staan centraal in Richtlijn (EU) 2019/713, met als hoofddoel iets te doen aan het feit dat Kaderbesluit 2001/413/JBZ niet langer de huidige realiteit weerspiegelt en een ontoereikende aanpak biedt van nieuwe uitdagingen en technologische ontwikkelingen, zoals virtuele valuta en mobiele betalingen. Deze moesten opgenomen worden om te zorgen voor een alomvattend antwoord op het fenomeen en om onbedoelde hiaten in de strafbaarstelling te dichten.

Het belangrijkste probleem bij de omzetting is de reikwijdte van virtuele valuta, zoals gedefinieerd in artikel 2, punt d), van de richtlijn. Hoewel elektronisch geld in alle lidstaten wordt gedefinieerd, vaak als gevolg van de omzetting van de richtlijn betreffende elektronisch geld[10], is de definitie en reikwijdte van virtueel geld niet altijd eenduidig.

[10] Richtlijn 2009/110/EG van het Europees Parlement en de Raad van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG (PB L 267 van 10.10.2009, blz. 7).

In HU wordt virtuele valuta beschouwd als eigendom en elektronische gegevens en kan ze als eigendom in beslag worden genomen of verbeurd verklaard. Op dezelfde manier is in PL virtuele valuta niet gedefinieerd in de wetgeving en er bestaat een zekere mate van onzekerheid over de vraag of ze zou vallen onder de verschillende strafbare feiten die relevant zijn voor de omzetting van de richtlijn, hoewel sommige auteurs van mening zijn dat virtuele valuta onder bepalingen van het wetboek van strafrecht zou kunnen vallen die betrekking hebben op strafbare feiten met betrekking tot informatie, gegevensdragers of informatiegegevens.

Veel lidstaten hebben deze definities omgezet door middel van financiële regels in plaats van in het strafrecht (AT, BE, BG, CY, CZ, DE, EE, EL, ES, HR, HU, LT, LU, LV, SI). Niet in al deze gevallen wordt echter verwezen naar de relevante bepalingen in de nationale wetgeving waarin de strafbare feiten zijn vastgelegd. Ten slotte zijn in drie lidstaten (IT, MT, RO) beide definities omgezet in het wetboek van strafrecht.

d) Informatiesysteem

In artikel 2, punt e), wordt "informatiesysteem" gedefinieerd door te verwijzen naar artikel 2, punt a), van Richtlijn 2013/40/EU. Alle lidstaten hebben de definitie in overeenstemming met de richtlijn omgezet.

e) Computergegevens

Computergegevens worden gedefinieerd in artikel 2, punt f), door te verwijzen naar artikel 2, punt b), van Richtlijn 2013/40/EU. Alle lidstaten hebben artikel 2, punt f), in overeenstemming met de richtlijn omgezet.

f) Rechtspersoon

Ten slotte wordt in artikel 2, punt g), "rechtspersoon" gedefinieerd. Bijna alle lidstaten hebben dit begrip in hun wetgeving omgezet. De enige uitzondering is SE, waar geen definitie van "rechtspersoon" wordt gegeven. Het begrip dat het dichtstbij komt en in de omzetting wordt gebruikt, is "onderneming". Dit begrip is echter niet gedefinieerd in enige wetstekst, noch in de rechtsleer of jurisprudentie.

2.2 Specifieke strafbare feiten

a) Frauduleus gebruik van niet-contante betaalinstrumenten

In artikel 3, punt a), van de richtlijn worden de lidstaten verplicht de nodige maatregelen te nemen om ervoor te zorgen dat frauduleus gebruik van een gestolen of anderszins wederrechtelijk toegeëigend of onrechtmatig verkregen niet-contant betaalinstrument, indien met opzet gepleegd, strafbaar wordt gesteld.

25 lidstaten hebben artikel 3, punt a), van de richtlijn omgezet. Van de 25 landen hebben 14 landen de richtlijn omgezet door middel van een bepaling die specifiek betrekking heeft op het frauduleus gebruik van niet-contante betaalinstrumenten (AT, CY, ES, FI, HU, IT, LT, MT, NL, PT, RO, SE, SI, SK). De overige lidstaten verwezen naar meer algemene strafbare feiten, zoals fraude en vervalsing met behulp van computers, of fraude in verband met betaalmiddelen, niet beperkt tot niet-contante betaalinstrumenten (BE, BG, CZ, DE, EE, EL, FR, HR, LU, LV, PL, SE, SK).

De wetgeving in HR verwijst niet naar het gebruik van gestolen of anderszins wederrechtelijk toegeëigende betaalinstrumenten; de omzettingsbepaling in HU heeft alleen betrekking op elektronische niet-contante betaalinstrumenten.

Volgens artikel 3, punt b), van de richtlijn nemen de lidstaten de nodige maatregelen om ervoor te zorgen dat frauduleus gebruik van een nagemaakt of vervalst niet-contant betaalinstrument, indien opzettelijk gepleegd, strafbaar wordt gesteld.

Artikel 3, punt b), is over het algemeen volledig omgezet.

Voor de omzetting van de richtlijn verwijzen 15 lidstaten naar nationale bepalingen inzake niet-contante betaalinstrumenten (AT, CY, DE, EE, ES, FI, HR, HU, IT, LT, MT, NL, PT, RO, SI), terwijl de nationale omzettingswetgeving in 10 lidstaten betrekking heeft op meer algemene strafbare feiten zoals diefstal of fraude, of strafbare feiten in verband met betaalinstrumenten, maar niet specifiek niet-contante instrumenten (BE, BG, CZ, EL, FR, LU, LV, PL, SE, SK).

b) Strafbare feiten in verband met het frauduleus gebruik van materiële niet-contante betaalinstrumenten

In artikel 4 van de richtlijn worden de lidstaten verplicht de nodige maatregelen te nemen om ervoor te zorgen dat de in de volgende alinea's opgesomde opzettelijk gepleegde handelingen strafbaar worden gesteld. In de alinea's worden genoemd: de diefstal of het zich anderszins wederrechtelijk toe-eigenen van een materieel niet-contant betaalinstrument in punt a); de frauduleuze namaak of vervalsing van een materieel niet-contant betaalinstrument in punt b); het bezit van een gestolen, anderszins wederrechtelijk toegeëigend, nagemaakt of vervalst materieel niet-contant betaalinstrument met het oog op het frauduleus gebruik ervan in punt c); de aanschaf voor zichzelf of een ander, waaronder de ontvangst, toe-eigening, aankoop, overdracht, invoer, uitvoer, verkoop, het vervoer of de verspreiding van een gestolen, nagemaakt of vervalst materieel niet-contant betaalinstrument met het oog op het frauduleus gebruik ervan in punt d).

Hoewel artikel 4 grotendeels op min of meer letterlijke wijze lijkt te zijn omgezet, roept de nationale omzetting in enkele gevallen vragen op als het gaat om de specifieke aanschaf voor zichzelf of een ander van een gestolen, nagemaakt of vervalst materieel niet-contant betaalinstrument met het oog op het frauduleus gebruik ervan.

c) Strafbare feiten in verband met het frauduleus gebruik van immateriële niet-contante betaalinstrumenten

In artikel 5 van de richtlijn worden gedragingen in verband met het frauduleus gebruik van immateriële niet-contante betaalinstrumenten strafbaar gesteld. Uit de analyse is gebleken dat dit artikel geen problemen lijkt te hebben veroorzaakt bij de omzetting. In de meeste gevallen is de nationale bepaling van toepassing op zowel materiële als immateriële niet-contante betaalinstrumenten. Iets minder dan de helft van de lidstaten heeft artikel 5 van de richtlijn omgezet in een meer algemene bepaling (BE, BG, DE, EE, FI, HR, FR, LV, PL, SE, SK), en iets meer dan de helft van hen heeft het artikel omgezet door middel van een bepaling die specifiek betrekking heeft op het frauduleus gebruik van niet-contante betaalinstrumenten (AT, CY, CZ, EL, ES, HU, IT, LT, LU, NL, PT, RO, SI).

d) Fraude met betrekking tot informatiesystemen

In artikel 6 van de richtlijn worden de lidstaten verplicht de nodige maatregelen te nemen opdat het overmaken, dan wel het bewerkstelligen van het overmaken van geld, monetaire waarde of virtuele valuta waardoor een andere persoon op ongeoorloofde wijze in zijn eigendom wordt aangetast, met het oogmerk een wederrechtelijk voordeel voor de dader of een derde te behalen, strafbaar wordt gesteld indien dit opzettelijk geschiedt door het onrechtmatig hinderen van of ingrijpen in de werking van een informatiesysteem (artikel 6, punt a)), of door het onrechtmatig invoeren, wijzigen, verwijderen, doorgeven of onderdrukken van computergegevens (artikel 6, punt b)). Alle lidstaten hebben artikel 6 omgezet.

e) Middelen voor het plegen van strafbare feiten

In artikel 7 van de richtlijn worden de lidstaten verplicht de nodige maatregelen te nemen opdat de vervaardiging, de aanschaf voor zichzelf of een ander, waaronder de invoer, uitvoer, verkoop, het vervoer of de verspreiding of het beschikbaar maken van een apparaat of instrument, computergegevens of enig ander middel dat hoofdzakelijk is ontworpen of specifiek geschikt is gemaakt voor het plegen van een van de in artikel 4, punten a) en b), artikel 5, punten a) en b), en artikel 6 bedoelde strafbare feiten, althans indien de feiten worden gepleegd met het oogmerk deze middelen daarvoor te gebruiken, strafbaar worden gesteld.

De overgrote meerderheid van de lidstaten heeft artikel 7 van de richtlijn in nationale wetgeving omgezet (AT, CY, CZ, DE, EE, ES, FI, FR, HR, IT, LT, LV, NL, RO, SE, SI, SK).

Zes landen hebben artikel 7 van de richtlijn omgezet door middel van bepalingen die verwijzen naar ruimere bepalingen, hetzij over algemene strafbare feiten zoals diefstal, hetzij betreffende financiële instrumenten en betaalmiddelen (BG, FI, FR, LV, SE, SK). Zeventien landen hebben de richtlijn omgezet door middel van een specifieke bepaling over instrumenten die worden gebruikt voor het plegen van de verschillende strafbare feiten van de richtlijn met betrekking tot materiële of immateriële niet-contante betaalinstrumenten (AT, CY, CZ, DE, EE, EL, ES, HR, HU, IT, LT, LU, MT, NL, PL, RO, SI).

Vijf lidstaten lijken problemen te hebben ondervonden bij de omzetting (BE, BG, HU, PL, PT).

2.3 Algemene regels voor de betreffende strafbare feiten

a) Uitlokking, medeplichtigheid en poging

Op grond van artikel 8, lid 1, van de richtlijn dienen de lidstaten de nodige maatregelen te nemen opdat uitlokking van en medeplichtigheid aan een in de artikelen 3 tot en met 7 bedoeld strafbaar feit strafbaar worden gesteld.

Alle lidstaten hebben deze bepaling omgezet. De overgrote meerderheid van de lidstaten heeft de richtlijn omgezet door middel van een reeds bestaand artikel over uitlokking en medeplichtigheid in het algemeen (AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SE, SI, SK). Twee lidstaten hebben echter besloten een nieuwe bepaling in te voeren, die alleen van toepassing is op de strafbare feiten van de richtlijn (CY, MT).

De lidstaten worden er in artikel 8, lid 2, eerste zin, van de richtlijn toe verplicht ervoor te zorgen dat poging tot het plegen van een in artikel 3, artikel 4, punt a), b) of d), artikel 5, punt a) of b), of artikel 6 bedoeld strafbaar feit, strafbaar wordt gesteld. Alle lidstaten lijken deze bepaling volledig te hebben omgezet, met uitzondering van BE, LU en SI.

Ook hier hebben de meeste lidstaten de richtlijn omgezet door middel van een reeds bestaande bepaling die van toepassing is op poging in het algemeen. (AT, BG, CZ, EE, EL, ES, FR, HR, HU, IT, LT, LV, NL, PL, PT, SE, SK). De overige lidstaten hebben het opgenomen in een speciale omzettingsmaatregel (CY, DE, FI, MT, RO).

Krachtens artikel 8, lid 2, tweede zin, moeten de lidstaten er ook voor zorgen dat op zijn minst een poging tot frauduleuze aanschaf van een onrechtmatig verkregen, nagemaakt of vervalst immaterieel niet-contant betaalinstrument, voor zichzelf of een ander (artikel 5, punt d)) strafbaar wordt gesteld.

Uit de evaluatie is gebleken dat de strafbaarstelling van poging in twee lidstaten onderworpen kan zijn aan beperkingen die niet in de richtlijn zijn opgenomen (HR, SI).

Alle overige lidstaten hebben de relevante bepalingen van de richtlijn omgezet. Dat deden ze ofwel door middel van een artikel over poging in het algemeen (AT, BE, BG, CZ, IT, EE, EL, ES, FR, HU, LT, LU, LV, NL, PL, PT, SE, SK), of door middel van een speciale omzettingsmaatregel (CY, DE, FI, MT, RO).

b) Sancties

In artikel 9 wordt bepaald dat de strafbare feiten in de artikelen 3 tot en met 8 kunnen worden bestraft met doeltreffende, evenredige en afschrikkende sancties, en wordt in de maximale gevangenisstraf voor de verschillende strafbare feiten voorzien.

Hoewel de lidstaten artikel 9 van de richtlijn over het algemeen hebben omgezet, bracht de evaluatie mogelijke problemen aan het licht met betrekking tot de reikwijdte van de definitie met betrekking tot artikel 9, lid 2, in HR en artikel 9, lid 6, in BE, CZ, HR en HU.

De vergelijking van de sancties die door de lidstaten voor de verschillende strafbare feiten zijn vastgesteld, is ingewikkeld omdat de strafbare feiten onder zowel algemene als specifieke bepalingen vallen. Bij de omzetting van de richtlijn door middel van bepalingen inzake algemene strafbare feiten hebben de lidstaten verschillende nationale bepalingen gebruikt om een van de door de richtlijn verboden handelingen strafbaar te stellen. Dit leidt tot verscheidene maximumsancties voor dat specifieke strafbare feit en impliceert dat de werkelijke maximumstraf zou afhangen van elk specifiek geval, van de aanpak die door de rechter wordt gevolgd en van nationale regels inzake samenloop van sancties. In PL geldt bijvoorbeeld de regel dat een handeling slechts één strafbaar feit kan opleveren. Indien een gedraging kenmerken vertoont die vallen onder twee of meer bepalingen van het strafrecht, moet de rechtbank één specifiek strafbaar feit kiezen. In BG daarentegen bepaalt de rechtbank in gevallen waarin het bijzondere deel van het wetboek van strafrecht voorziet in het gelijktijdig opleggen van twee of meer sancties voor een bepaald strafbaar feit, de omvang van elke sanctie zodanig dat de optelling ervan strookt met de algemene doelstellingen van de straf.

Bovendien kunnen bepalingen verzwarende omstandigheden bevatten die het plafond kunnen verhogen en tot hogere sancties kunnen leiden. De maximale straf is dus afhankelijk van de manier waarop het strafbare feit is gepleegd. De algemene bepaling inzake verduistering in HR bevat bijvoorbeeld een maximale gevangenisstraf van vijf jaar. Als de dader echter geweld gebruikt, is de maximumstraf tien jaar, en als de handeling heeft geleid tot een aanzienlijke materiële winst, kan de dader maximaal twaalf jaar gevangenisstraf krijgen. In DE leidt het vervalsen van materiële niet-contante betaalinstrumenten tot een maximale gevangenisstraf van vijf jaar. Als de dader echter handelde uit winstbejag, bedraagt de straf maximaal tien jaar.

Uit de evaluatie bleek ook dat in de meeste gevallen de drempels in de nationale wetgeving strenger zijn dan die van de richtlijn. Het verschil kan aanzienlijk zijn: op valsemunterij staat in BG en LU een maximale gevangenisstraf van 15 jaar en in PL maximaal 25 jaar. Slechts twee lidstaten voorzien in gelijke (of bijna gelijke) maximumstraffen als die van de richtlijn (AT, MT).

c) Aansprakelijkheid van rechtspersonen

Uit de evaluatie bleek dat zestien lidstaten artikel 10 van de richtlijn hebben omgezet op basis van een reeds bestaande algemene bepaling van hun wetboek van strafrecht (AT, CZ, BE, BG, DE, EE, ES, FR, HR, HU, LU, LV, NL, PT, RO, SE), terwijl negen lidstaten het in het kader van de richtlijn hebben omgezet door middel van een wet die specifiek betrekking heeft op de aansprakelijkheid van rechtspersonen (CY, EL, FI, IT, LT, MT, PL, SI, SK).

d) Sancties voor rechtspersonen

In artikel 11 van de richtlijn worden de lidstaten verplicht om ook voor rechtspersonen doeltreffende, evenredige en afschrikkende sancties vast te stellen, die al dan niet strafrechtelijke boeten omvatten. Alle lidstaten hebben dergelijke sancties ingevoerd.

In artikel 11 wordt de lidstaten de mogelijkheid geboden om verschillende specifieke sancties op te nemen voor rechtspersonen, zoals de uitsluiting van het recht op door de overheid verleende uitkeringen of gerechtelijke ontbinding. Zes lidstaten hebben helemaal geen gebruik gemaakt van de mogelijkheid die in artikel 11 van de richtlijn is opgenomen (AT, BG, EE, FI, NL, SE). De overige negentien landen hebben artikel 11 geheel of gedeeltelijk in nationale wetgeving omgezet (BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LT, LU, LV, MT, PL, PT, RO, SI, SK).

e) Rechtsmacht

In dit artikel worden de lidstaten verplicht hun rechtsmacht vast te stellen voor strafbare feiten die op hun grondgebied of door een onderdaan zijn gepleegd; dit is in alle lidstaten omgezet in de algemene bepalingen van het nationale wetboek van strafrecht of strafvordering. Daarom zijn het territorialiteitsbeginsel en het actief nationaliteitsbeginsel algemeen van toepassing en niet specifiek voor de strafbare feiten die in deze richtlijn worden geregeld. Daarnaast werd artikel 12 ook door CY omgezet in de nationale wet inzake de bestrijding van fraude en vervalsing van niet-contante betaalmiddelen en door PT in de wet inzake cybercriminaliteit.

Alle lidstaten hebben artikel 12, lid 1, punten a) en b), in nationale wetgeving omgezet.

Op grond van artikel 12, lid 3, kunnen de lidstaten rechtsmacht vestigen ten aanzien van een in de artikelen 3 tot en met 8 van de richtlijn bedoeld strafbaar feit dat buiten hun grondgebied is gepleegd, indien, onder meer, a) het strafbaar feit is gepleegd door iemand die zijn gewone verblijfplaats op hun grondgebied heeft; b) het strafbaar feit is gepleegd ten voordele van een op zijn grondgebied gevestigde rechtspersoon; of c) het strafbaar feit is gepleegd jegens een eigen onderdaan of een persoon die zijn vaste woon- of verblijfplaats op zijn grondgebied heeft. Veertien lidstaten (BE, CY, CZ, DE, EL, ES, FI, HR, LT, LV, MT, NL, SE, SK) hebben gebruik gemaakt van de mogelijkheid in artikel 12, lid 3, punt a); twaalf lidstaten (BE, CY, CZ, EL, FI, LV, MT, NL, PL, PT, SI, SK) hebben artikel 12, lid 3, punt b), in nationale wetgeving omgezet; en zestien lidstaten (AT, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, LV, MT, RO, SE, SI) hebben hun rechtsmacht uitgebreid overeenkomstig artikel 12, lid 3, punt c). Met betrekking tot dit punt c) is in BG, DE, EE, HU, RO en SI rechtsmacht vastgesteld voor een strafbaar feit dat buiten hun grondgebied is gepleegd en waarbij het strafbaar feit (uitsluitend) tegen een van de eigen onderdanen is gepleegd, waardoor personen met vaste woon- of verblijfplaats op hun grondgebied zijn weggelaten. AT voorziet in vervolging door het Oostenrijkse strafrechtsysteem voor in het buitenland gepleegde strafbare feiten indien de dader en het slachtoffer Oostenrijkers zijn. CY, CZ, EL, FI, LV en MT hebben gebruik gemaakt van alle drie optionele bepalingen van artikel 12, lid 3.

2.4 Operationele kwesties

a) Doeltreffende opsporing en samenwerking

In alle lidstaten zijn opsporingsmiddelen voor het onderzoeken en vervolgen van de in de artikelen 3 tot en met 8 bedoelde strafbare feiten niet expliciet opgenomen in de wetgeving tot omzetting van de richtlijn, maar eerder in meer algemene wetgeving, zoals in het wetboek van strafvordering. Doorgaans houdt de mogelijkheid om in een bepaald geval een opsporingsmiddel te gebruiken verband met de sanctie voor het betreffende strafbare feit; zoals reeds wordt aangegeven in de bepaling van de richtlijn, zullen de opsporingsmiddelen die in de strijd tegen georganiseerde of andere zware criminaliteit worden ingezet, ook beschikbaar zijn voor het onderzoeken en vervolgen van de strafbare feiten die in deze richtlijn zijn opgesomd. De uitzonderlijkheid van bepaalde opsporingsmiddelen en de noodzaak van evenredigheid met het strafbare feit worden meestal opgenomen in de relevante wettelijke bepalingen en/of in de Grondwet.

Overeenkomstig artikel 13, lid 2, van de richtlijn moet informatie over de in de artikelen 3 tot en met 8 bedoelde strafbare feiten onverwijld ter kennis worden gebracht van de autoriteiten die die strafbare feiten opsporen of vervolgen. Met andere woorden, rechtshandhavingsautoriteiten en andere bevoegde autoriteiten moeten tijdig toegang tot relevante informatie hebben voor de opsporing en vervolging van de in deze richtlijn bedoelde strafbare feiten (overweging 22). Het wetboek van strafvordering voorziet vaak in verschillende meldingssystemen, zodat strafbare feiten (in de zin van de artikelen 3 tot en met 8 van de richtlijn) efficiënt en snel kunnen worden gemeld. Deze meldingssystemen omvatten: een meldingsplicht voor overheidsinstanties en autoriteiten; een klokkenluiderssysteem; een klachtenprocedure; een verplichting voor betalingsdienstaanbieders om ernstige operationele of beveiligingsincidenten te melden; en een recht van particulieren om incidenten te melden. Verder kunnen bepaalde meer specifieke wetten ervoor zorgen dat meldingen van beveiligingsincidenten (waaronder meldingen van ernstige strafbare feiten, zoals ongeoorloofde verkrijging, vervalsing en wijziging van een betaalmiddel) zo snel mogelijk aan de relevante autoriteiten worden gemeld. Dergelijke wetten zijn gerapporteerd door AT, CZ, LT, FI, MT en PT.

De voorwaarde dat de ingediende informatie “de relevante autoriteiten onverwijld ter kennis wordt gebracht” wordt meestal niet expliciet omgezet.

b) Informatie-uitwisseling

De uitwisseling van informatie tussen nationale rechtshandhavingsautoriteiten ten behoeve van de opsporing en vervolging van misdrijven, waaronder de in de artikelen 3 tot en met 8 van de richtlijn bedoelde strafbare feiten, kan worden vergemakkelijkt door middel van operationele contactpunten (overweging 26). In artikel 14, lid 1, eerste zin, van de richtlijn worden de lidstaten verplicht deze contactpunten inderdaad in te stellen en dat ze 24/7 beschikbaar zijn. Verder worden de lidstaten er in de tweede zin toe verplicht om over procedures te beschikken om dringende verzoeken om bijstand snel in behandeling te nemen en binnen acht uur na het verzoek te reageren, waarbij ten minste wordt aangegeven of het verzoek in behandeling zal worden genomen, alsmede de vorm van een dergelijk antwoord en het tijdstip waarop dit naar verwachting zal gebeuren.

De volgende lidstaten hebben besloten gebruik te maken van een bestaand operationeel contactpunt voor de in deze richtlijn beschreven doeleinden: AT, BE, CY, EE, EL, ES, FR, HU, IT, LT, LV, NL, PL, PT, SE.

Tabel 1 bevat een overzicht van de vastgestelde contactpunten. In BG, CZ, LU, SI, HR zijn geen contactpunten bekend.

Tabel 1 Operationele contactpunten

LS	Contactpunt	LS	Contactpunt
AT	Federale gerechtelijke politie	**EE**	Ministerie van Justitie
BE	Directie van de internationale politiesamenwerking	**FI**	Nationaal inlichtingenbureau
BG	Niet bekend	**FR**	Afdeling voor internationale betrekkingen van de centrale directie van de gerechtelijke politie
CY	Politie van Cyprus	**HR**	Niet bekend
CZ	Niet bekend	**HU**	Internationaal centrum voor strafrechtelijke samenwerking (NEBEK)
DE	16 politiebureaus van de deelstaten en één federaal politiebureau, centrale contactpunten voor cybercriminaliteit	**MT**	Politiemacht van Malta
EL	Griekse politie (afdeling internationale politiesamenwerking)	**ES**	Eenheid voor noodcoördinatie
IT	Afdeling Internationale operaties van de Dienst voor internationale politiesamenwerking	**NL**	Landelijk Internationaal Rechtshulpcentrum (LIRC)
LT	Tweede afdeling van het bestuur van de Afdeling Politie onder het ministerie van Binnenlandse Zaken van de Republiek Litouwen en de raad voor internationale betrekkingen van de gerechtelijke politie in Litouwen	**PL**	Hoofdbureau van de algemene politie
LV	Nationale politie	**PT**	Gerechtelijke politie
RO	Afdeling vervolging en strafrechtelijk onderzoek van het openbaar ministerie	**SE**	Politie-autoriteit
SI	Niet bekend	**SK**	Dienst Gerechtelijke Politie van het presidium van de politie van de Slowaakse Republiek

Het bepaalde in artikel 14, lid 1, tweede zin, van de richtlijn is in enkele lidstaten praktisch uitgevoerd. Informatie over de procedures die van toepassing zijn op dringende verzoeken, is niet gevonden in BE, BG, CZ, LV, RO, FR, HR, LU, NL, PL, SE, SK.

c) Melding van misdrijven

De lidstaten zijn ook verplicht om passende meldkanalen beschikbaar te stellen. Dergelijke kanalen om vermoedelijke fraude te melden of, meer in het algemeen, om mogelijke strafbare feiten te melden, kunnen in wetgeving worden vastgelegd. Vaak hebben de lidstaten het melden van een misdrijf vastgesteld als een verplichting voor bepaalde categorieën (natuurlijke personen en rechtspersonen) (grotendeels in overeenstemming met artikel 15, lid 2), terwijl slachtoffers en andere "omstanders" de mogelijkheid krijgen (maar niet verplicht zijn) om aangifte te doen. Deze wettelijke bepalingen worden gewoonlijk aangevuld met praktische uitvoeringsmaatregelen.

In alle lidstaten kan schriftelijk of mondeling melding worden gedaan bij de politie en/of de rechterlijke macht. Daarnaast hebben sommige lidstaten aanvullende meldkanalen beschikbaar gesteld:

De federale wetgeving in AT voorziet in verschillende meldingssystemen, zodat strafbare feiten in de zin van de artikelen 3 tot en met 8 van de richtlijn efficiënt en snel kunnen worden gemeld: 1) de meldingsplicht voor overheidsinstanties en autoriteiten; 2) het klokkenluiderssysteem van het centraal bureau van het Openbaar Ministerie voor de vervolging van economische criminaliteit en corruptie; 3) het klokkenluiderssysteem van de toezichthoudende autoriteit voor de financiële markt; en 4) de verplichting voor betalingsdienstaanbieders om ernstige operationele of beveiligingsincidenten te melden. Bij de federale recherche-informatiedienst is een specifiek meldpunt voor cybercriminaliteit opgericht. Daarnaast werkt het federale ministerie van Binnenlandse Zaken samen met de federale economische kamer. Dit heeft geleid tot verschillende mailings en campagnes om het publiek te motiveren en aan te moedigen om relevante overtredingen van de wet te melden.

In BE beheert het ministerie van Economische Zaken één aanspreekpunt voor slachtoffers van misleiding, bedrog, fraude en oplichting. Daarnaast is er wettelijk een klokkenluiderskanaal opgericht dat door de Autoriteit voor Financiële Diensten en Markten beschikbaar is gesteld voor alle klachten met betrekking tot krediet- of beleggingsproducten en -diensten.

In CY zijn de Cypriotische politie, samen met de centrale bank van Cyprus en de nationale autoriteit voor de beveiliging van netwerk- en informatiesystemen door middel van een wetgevende maatregel formeel aangewezen als de bevoegde nationale autoriteiten die verantwoordelijk zijn voor het opzetten van passende meldings- en communicatiekanalen.

Het strafrecht in CZ verplicht overheidsinstanties om aangifte te doen.

In DE moeten meldingsplichtige entiteiten verdachte transacties onverwijld melden. Daarnaast zijn op federaal niveau niet-wetgevende maatregelen genomen, zoals een geïnstitutionaliseerd publiek-privaat partnerschap met het oog op het vaststellen, voorkomen, opsporen of vervolgen van de in de artikelen 3 tot en met 8 van de richtlijn bedoelde strafbare feiten, en een platform voor de uitwisseling van informatie.

In EL heeft de Griekse regering, naast de algemene meldkanalen, een online overheidsdienst opgezet waar burgers rechtstreeks klachten kunnen indienen over online gepleegde strafbare feiten. Bovendien moeten kredietinstellingen en andere aanbieders van betalingsdiensten elke vorm van fraude onmiddellijk melden aan de Bank van Griekenland (die bevoegd is om dergelijke klachten te behandelen).

In ES biedt de Bank van Spanje niet alleen algemene meldkanalen, maar ook meldkanalen aan in samenwerking met het nationale instituut voor cyberbeveiliging.

In de Italiaanse wetgeving is vastgelegd dat de politie tijdig informatie over een strafbaar feit aan de openbare aanklager moet doorgeven, die op eigen initiatief of naar aanleiding van een aangifte of een rechtszaak is verkregen. Het delen van informatie via digitale platforms wordt ook aangemoedigd.

LT beschikt over meerdere meldkanalen om de in de artikelen 3 tot en met 8 van de richtlijn bedoelde strafbare feiten te melden, via een internetpagina (e-politieportaal), via het algemene noodtelefoonnummer 112, persoonlijk, per e-mail, per sms en via de mobiele applicatie e-politie, en andere automatische middelen. Betalingsdienstaanbieders, financiële instellingen en andere meldingsplichtige entiteiten, de Bank van Litouwen en de opsporingsdienst voor financiële delicten zijn verplicht om de bevoegde rechtshandhavingsautoriteiten in kennis te stellen van redelijke vermoedens van criminele en/of andere onrechtmatige handelingen.

In LU is een website beschikbaar waarin wordt uitgelegd hoe fraude kan worden gemeld. De toezichtscommissie voor de financiële sector heeft richtsnoeren opgesteld om financiële fraude op te sporen, maar verzoekt ook alle instellingen onder haar toezicht om fraude en incidenten als gevolg van externe computeraanvallen zo snel mogelijk te melden.

In RO bestaat er een meldingsplicht voor ambtenaren en personen die leidinggevende functies bekleden binnen overheidsinstanties, personen die diensten van openbaar belang verrichten en personen die optreden in controle- en toezichtsorganen.

In SI zijn alle overheidsinstanties en organisaties met openbaar gezag verplicht om strafbare feiten te melden.

Het Perceval-platform in FR, opgericht bij wet, biedt slachtoffers de mogelijkheid om melding te maken van fraude met bankkaarten en vervalsing. Er bestaat een soortgelijk platform voor het melden van cybercriminaliteit. Verder zijn sancties van toepassing op elke natuurlijke of rechtspersoon die door niet onmiddellijk actie te ondernemen, een misdrijf niet voorkomt, hetgeen leidt tot een algemene meldingsplicht.

In HU geldt de verplichting om een strafbaar feit te melden alleen voor autoriteiten, overheidsfunctionarissen en leden van wettelijke beroepsorganisaties. Op haar website moedigt de Hongaarse nationale bank, in de vorm van een advies, financiële instellingen aan om vermoedelijke fraude te melden.

In MT moedigt het nationale contactpunt met name financiële instellingen aan om melding te maken van vermoedelijke fraude en vervalsing van niet-contante betaalmiddelen.

In PT is er naast het wettelijk opgerichte meldkanaal voor klokkenluiders een eenvoudig te benaderen meldingssysteem voor cybercriminaliteit beschikbaar, waar een link gevolgd kan worden die onmiddellijk een aan de bevoegde autoriteiten gerichte e-mail opent.

In SE kunnen bepaalde soorten criminaliteit, zoals creditcardfraude, ook via de e-dienst van de politie worden gemeld. Ook zijn organisaties die zich bezighouden met bank- en financieringsactiviteiten, verplicht om verdachte activiteiten in verband met mogelijke gevallen van witwassen of van financiering van terrorisme, of in verband met vermogen dat anderszins voortkomt uit een strafbaar feit, aan de politie te melden. Daarnaast wordt er een voortdurende dialoog gevoerd tussen het bankwezen en de financiële sector en het nationale fraudecentrum van de politie.

De wettelijke bepalingen in SK bevatten een verplichting (en procedures) voor overheidsinstanties en andere rechtspersonen om strafbare feiten onmiddellijk aan de rechtshandhavingsautoriteiten te melden. Meldingsplichtige personen en in het bijzonder banken hebben een meldingsplicht met betrekking tot witwassen.

Als alternatief hebben NL en PL met niet-wetgevende maatregelen uitvoering gegeven aan artikel 15 van de richtlijn. De Nederlandse politiediensten en de website van de politie bieden een passend kanaal om fraude met niet-contante betaalmiddelen aan de autoriteiten te melden. Verder heeft de Nederlandse overheid toegezegd financiële instellingen en andere rechtspersonen aan te moedigen elk vermoeden van fraude te melden. Deze inspanning blijkt bijvoorbeeld uit het bestaan van een Frontoffice Fraude Financieel bij alle politie-eenheden in Nederland. Ook hebben vier grote banken en ICS-creditcards een convenant gesloten met de politie om gezamenlijk (bank)fraude en phishing te bestrijden. In PL worden meldingen van misdrijven 24/7 door alle politie-eenheden geaccepteerd. Vanwege de aard van de misdrijven die met behulp van computertechnologieën worden gepleegd, is het bovendien mogelijk om rechtstreeks contact op te nemen met een gespecialiseerde organisatorische eenheid van het hoofdkwartier van de politie. Om te zorgen voor een zo snel mogelijke samenwerking met de banksector is bovendien een samenwerkingskanaal opgericht tussen het bureau voor de bestrijding van cybercriminaliteit van het politiebureau en het bankbeveiligingscentrum van de Poolse bankenvereniging.

In BG, EE en HR is artikel 15, lid 2, van de richtlijn niet omgezet.

2.5 Ondersteuning van slachtoffers en preventie

a) Bijstand en ondersteuning aan slachtoffers

In artikel 16, lid 1, van de richtlijn wordt de bijstand en ondersteuning aan natuurlijke personen en rechtspersonen van wie persoonsgegevens zijn misbruikt, gewaarborgd. Hierbij moet het gaan om: a) het verstrekken van specifieke informatie en specifiek advies over bescherming tegen de negatieve gevolgen van dergelijke misdrijven, en b) het verstrekken van een lijst van instellingen die zich specifiek bezighouden met de verschillende aspecten van identiteitsfraude en ondersteuning aan slachtoffers.

In dezelfde geest moeten rechtspersonen die het slachtoffer zijn van de in de artikelen 3 tot en met 8 van deze richtlijn bedoelde strafbare feiten, toegang hebben tot informatie over a) de procedures voor het indienen van een klacht, b) het recht om informatie te ontvangen over de zaak, c) de beschikbare procedures voor het indienen van een klacht indien de bevoegde autoriteit de rechten van het slachtoffer tijdens een strafprocedure niet eerbiedigt, en d) de contactgegevens voor communicatie over hun zaak (artikel 16, lid 3, van de richtlijn).

Het wetboek van strafvordering van de meeste lidstaten bevat voorschriften over slachtoffers en hun rechten, waaronder enkele specifieke bepalingen over het recht van slachtoffers op informatie en bijstand tijdens procedures, het recht op begeleiding en het recht om een klacht in te dienen. Een specifieke wet tot omzetting van de richtlijn vormt vaak een aanvulling op wat al is vastgelegd in het wetboek van strafvordering. Rechtspersonen worden doorgaans behandeld in afzonderlijke wettelijke bepalingen in het wetboek van strafvordering of elders. Daarnaast zijn er verschillende informatiecampagnes, folders, speciale websites, circulaires enz. beschikbaar om slachtoffers van de in de artikelen 3 tot en met 8 van de richtlijn bedoelde strafbare feiten bij te staan en te ondersteunen. Dit is het geval in AT, BE (met betrekking tot artikel 16, lid 1), CY, CZ, DE, IT, LT, LU (met betrekking tot artikel 16, lid 1), LV (met betrekking tot artikel 16, lid 3), RO, SI (met betrekking tot artikel 16, lid 3), EE, FI (met betrekking tot artikel 16, lid 1), FR (met betrekking tot artikel 16, lid 1), HR, HU, NL, PL (met betrekking tot artikel 16, lid 3), PT, SE en SK. Artikel 16, lid 1, en artikel 16, lid 3, van de richtlijn zijn nergens letterlijk of bijna letterlijk omgezet, met uitzondering van MT.

De lijst van erkende centra voor slachtofferhulp, zoals bedoeld in artikel 16, lid 1, punt b), van de richtlijn, is meestal online beschikbaar en wordt daarom in de praktijk uitgevoerd.

b) Preventie

Artikel 17 heeft betrekking op preventie en in dit artikel wordt vereist dat de lidstaten passende maatregelen nemen, zoals voorlichtings- en bewustmakingscampagnes en onderzoeks- en onderwijsprogramma's. Dit onderdeel is gebaseerd op een beoordeling van de informatie die door de lidstaten aan de Commissie is verstrekt en op een open online bronnenonderzoek om het bestaan van preventiemaatregelen te onderzoeken. Zoals beschreven in tabel 2 hieronder, hebben de aangetroffen preventiemaatregelen voornamelijk betrekking op cybercriminaliteit en onlinefraude. In bepaalde landen wordt echter ook informatie over fraudepreventie verstrekt, meestal door de politie.

Tabel 2 Preventie-activiteiten

LS	Activiteiten
AT	De federale politie verstrekt regelmatig informatie op haar website en in sociale netwerken over manieren om zich tegen fraude te beschermen. Samenwerking met belanghebbenden zoals de Kamer van Koophandel wordt ondersteund en uitgevoerd in het kader van e-commerceprojecten.
BE	Verschillende websites met advies/bewustmakingsmateriaal, zoals die van het Centrum voor Cybersecurity België (CCB). Bepaalde vormen van samenwerking met belanghebbenden kunnen worden vastgesteld door middel van zoeken op internet; zo heeft de organisatie die de financiële sector vertegenwoordigt, samengewerkt met het Brussels parket om bewustmakingsmateriaal te ontwikkelen.
BG	In Bulgarije is in 2021 een campagne tegen "geldezels" gestart door de vereniging van banken, die is uitgevoerd in samenwerking met de algemene directie voor bestrijding van georganiseerde misdaad en het openbaar ministerie. De algemene directie is ook een campagne tegen phishing gestart.
CY	De afdeling cybercriminaliteit van de politie biedt op haar website informatie en advies over zaken als digitale fraude en informatie over aankomende evenementen, zoals bewustmakingscampagnes. Een voorbeeld hiervan is de voorlichtingscampagne over informatiebeveiliging, uitgevoerd door de politie, de centrale banken, de bankenvereniging en de autoriteit voor digitale beveiliging.
DE	De federale recherchedienst (BKA) biedt op haar website een overzicht van de maatregelen gericht op geïnstitutionaliseerde publiek-private samenwerking met het oog op het opsporen, voorkomen, onderzoeken of vervolgen van de strafbare feiten die onder de richtlijn vallen, bijvoorbeeld het partnerschap tussen de federale recherchedienst (BKA), het federale bureau voor informatiebeveiliging (BSI) en het Duitse kenniscentrum tegen cybercriminaliteit (G4C), een vereniging van financiële instellingen en bedrijven uit de IT-beveiligingssector. Het BKA heeft ook de Cybercrime Conference C³ opgezet, een platform voor uitwisseling tussen autoriteiten, het bedrijfsleven, de wetenschap en de politiek. Het G4C stelt ook informatiebrochures op en stelt trainingen samen. Ten slotte neemt het BKA ook deel aan preventiemaatregelen op het gebied van

	cybercriminaliteit in de deelstaten en op nationaal niveau werkt het BKA ook samen met andere politie- en niet-politieautoriteiten en -organisaties (belanghebbenden) en intensiveert het de samenwerking, met name op het gebied van onderwerpen die in de belangstelling staan.
FR	Het ministerie van Binnenlandse Zaken publiceert informatie over cyberpreventie. Tot de beschikbare platforms voor het melden van cybercriminaliteit behoren ook preventieberichten en de informatie- en communicatiedienst van de nationale politie (SICoP). Andere voorbeelden zijn de richtlijnen van de Bank van Frankrijk of de door de nationale taskforce voor fraudebestrijding gepubliceerde gids over fraudepreventie, waarin verschillende bestuurlijke en handhavingsautoriteiten zijn samengebracht.
EL	De afdeling cybercriminaliteit en de landelijke politie zijn zeer actief in het informeren van het publiek, bewustmaking en het verminderen van het risico om slachtoffer te worden van fraude, met tv-campagnes, educatieve activiteiten en online informatie.
ES	Het Spaanse nationale cyberbeveiligingsinstituut en de belastingdienst verstrekken op hun website relevante informatie om phishing, ransomware enz. in zakelijke omgevingen te voorkomen.
HR	Het ministerie van Binnenlandse Zaken biedt online informatie over internetfraude en beheert een YouTube-kanaal over fraude en computerbeveiliging, met video's over cyberoplichting.
IT	Het ministerie van Financiën, dat tot taak heeft fraude met betaalmiddelen te voorkomen, stimuleert al een reeks initiatieven op lokaal niveau, in samenwerking met lokale overheden en het universitaire systeem, en organiseert seminars en workshops gericht op de risicogroepen bij vervalsing van valuta, waaronder burgers.
LT	Informatie over preventie met betrekking tot online fraude is te vinden op de website van de toezichthoudende autoriteit op het gebied van telecommunicatie; op de website van de politie staat informatie over de meest voorkomende soorten cyberfraude. Daarnaast is een van de doelstellingen van de nationale strategie inzake cybercriminaliteit het versterken van de preventie en beheersing van cybercriminaliteit, met name door het ontwikkelen van een effectieve samenwerking tussen rechtshandhavingsautoriteiten en andere belanghebbenden.
LV	De commissie voor financiële en kapitaalmarkten heeft verschillende internettools ontwikkeld om informatie en begeleiding te bieden over financiële veiligheid en fraudekwesties. Daarnaast zijn er verschillende campagnes georganiseerd in samenwerking met de nationale politie en het centrum voor consumentenbescherming.
NL	Er zijn maatregelen getroffen, zoals de Fraudehelpdesk, een organisatie die wordt gesubsidieerd door de Nederlandse overheid. Bij de Fraudehelpdesk kunnen frauduleuze acties worden gemeld, en de organisatie maakt deel uit van de stichting SAFECIN (Stichting aanpak financieel-economische Criminaliteit in Nederland), een stichting met betrokkenheid van de overheid.
SE	Er wordt een voortdurende dialoog gevoerd tussen het bankwezen en de financiële sector en het nationale fraudecentrum van de politie (NBC). Daarnaast werkt het NBC samen met bijvoorbeeld marktdeelnemers in de e-commerce, ook voor misdaadpreventie. Het belang van het melden van fraude bij de politie wordt in deze contacten benadrukt.

Voor tien lidstaten (CZ, EE, FI, HU, MT, PL, PT, RO, SI, SK) is geen informatie gevonden over passende preventiemaatregelen en de praktische uitvoering daarvan, hoewel in MT en RO de wetgeving deze verplichting wel omvat en de formulering van de richtlijn nauwgezet volgt.

3. Conclusies en volgende stappen

De richtlijn heeft tot aanzienlijke vooruitgang geleid in het op een vergelijkbaar niveau strafbaar stellen van fraude met en vervalsing van niet-contante betaalmiddelen in de lidstaten, wat de grensoverschrijdende samenwerking van autoriteiten op het gebied van wetshandhaving die dit soort strafbare feiten onderzoeken, gemakkelijker maakt. De lidstaten hebben strafwetboeken en andere relevante wetgeving gewijzigd, procedures gestroomlijnd en samenwerkingsprogramma's opgezet of verbeterd. De Commissie is zich ervan bewust dat de lidstaten grote inspanningen hebben geleverd om de richtlijn om te zetten.

De richtlijn heeft nog meer potentieel, maar om dat te kunnen waarmaken zouden de lidstaten alle bepalingen ervan volledig ten uitvoer moeten brengen. Uit de analyse tot dusver blijkt dat

enkele van de belangrijkste door de lidstaten te bereiken verbeteringen, onder meer omvatten: artikel 2, punt d), dat de definitie van virtuele valuta bevat; artikel 7 inzake strafbare feiten die verband houden met de middelen die zijn gebruikt voor het plegen van de strafbare feiten, en artikel 8, lid 2, over pogingen tot strafbare feiten; artikel 9, lid 6, inzake de strafbaarstelling voor natuurlijke personen in het geval dat het strafbare feit is gepleegd in het kader van een criminele organisatie; artikel 14 over de uitwisseling van informatie; en artikel 16 over bijstand en ondersteuning aan slachtoffers.

De Commissie zal de lidstaten ondersteuning blijven bieden bij de uitvoering van de richtlijn. In het bijzonder zal in 2023 een oproep tot het indienen van voorstellen hiertoe worden gepubliceerd.

De Commissie is vastbesloten ervoor te zorgen dat de omzetting in de hele EU wordt afgerond en dat de bepalingen correct worden uitgevoerd. Dit houdt onder meer in dat zij erop zal toezien dat de nationale maatregelen voldoen aan de overeenkomstige bepalingen in de richtlijn. Zo nodig zal de Commissie haar handhavingsbevoegdheden uit hoofde van de Verdragen aanwenden door inbreukprocedures in te leiden.