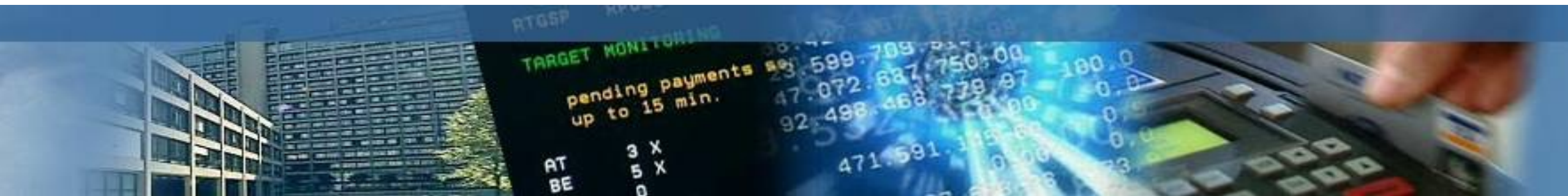


Prävention und Risiko-Management Betrug im Massenzahlungsverkehr aus Zentralbanksicht

Dirk Schrade



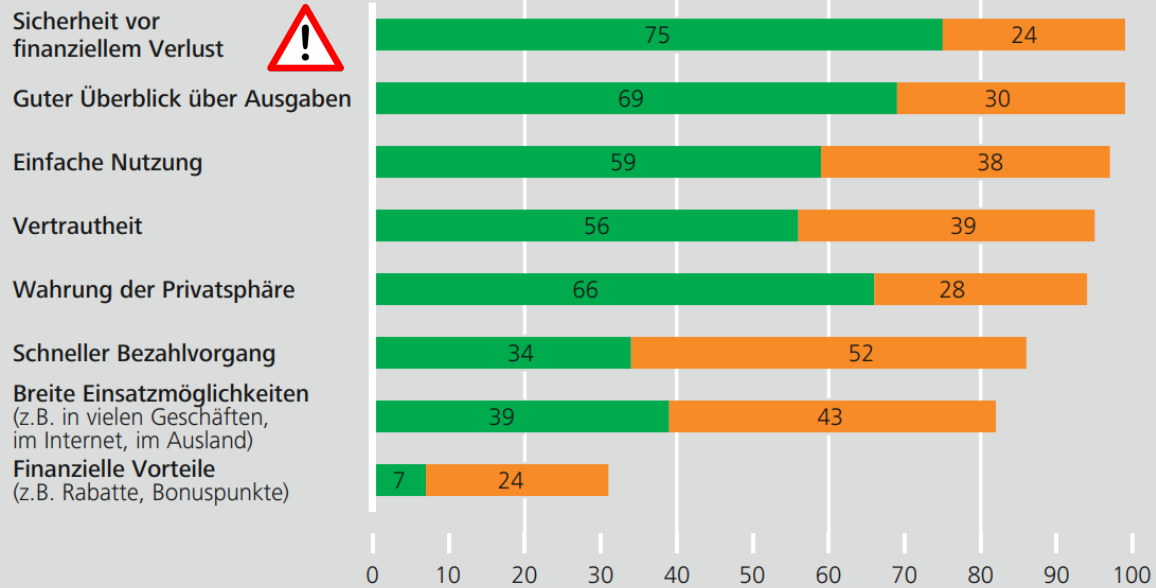
Relevanz von Sicherheit im Zahlungsverkehr

Sicherheit aus Nutzersicht

Anforderungen an Zahlungsmittel

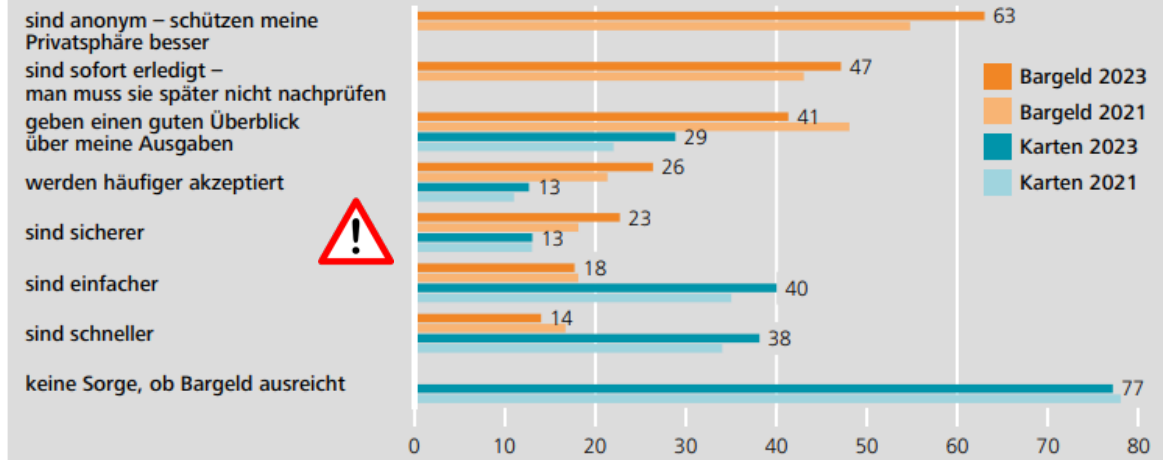
2017, Angaben in %, gemäß Selbstausskunft der Befragten

Frage: Wie wichtig ist Ihnen die jeweilige Eigenschaft bei einem Zahlungsmittel? ¹⁾



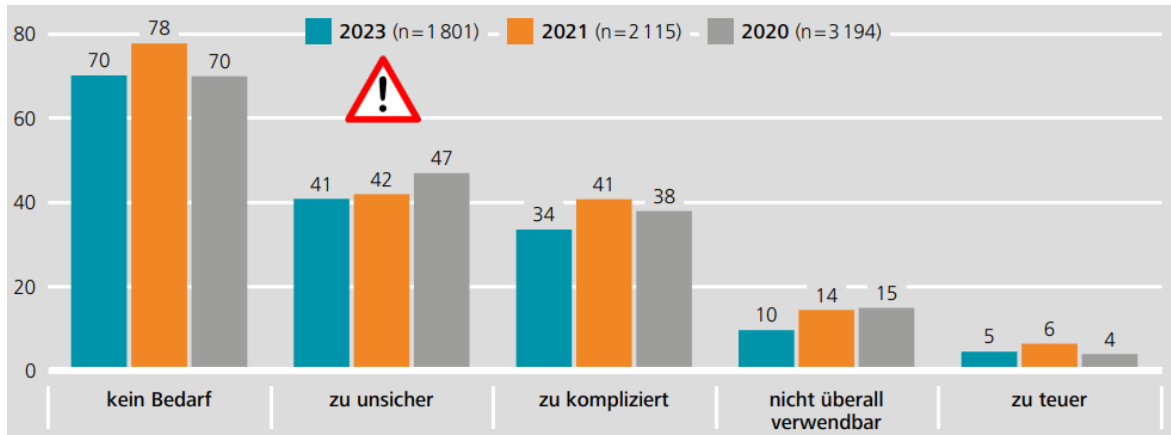
Vorteile von Barzahlungen / Kartenzahlungen im direkten Vergleich

in %, gemäß Selbstausskunft, Mehrfachnennungen möglich



Gründe für die Nichtnutzung mobiler Bezahlverfahren

in %, gemäß Selbstausskunft, Mehrfachnennungen möglich



Relevanz von Sicherheit im Zahlungsverkehr

Sicherheit als strategisches Aufgabenfeld



Quelle: Eigene Illustration nach istock-Vorlage

Nationale Zahlungsverkehrsstrategie - Irland

Future role for cash

Future outcome 3.1: All government departments and bodies under their aegis to accept electronic payments and cash payments (or facilitate cash payments).

Future outcome 3.2: To ensure all sectors of the economy are aware of the forthcoming EU legal tender regulation and their obligations regarding mandatory cash acceptance (if applicable), along with potential changes they may need to make to accommodate this and any other relevant issues arising from the regulation.

Future outcome 3.3: There will be a comprehensive overview of the national cash cycle environment that will inform policy thinking and formation in relation to cash and payments.

Resilience of payments

Future outcome 4.1: There are appropriate system-wide contingency arrangements to prepare for and manage disruptions to payment services.

Future outcome 4.2: The Central Bank will have appropriate powers to ensure relevant firms leave the market in an orderly manner.

Future outcome 4.3: A safe and easy to use EU-certified digital identify wallet will be available.

Payment fraud

Future outcome 5.1: Greater anti-fraud information sharing in the Irish banking sector.

Future outcome 5.2: Illegal online content flagged by the financial services industry will be prioritised for review by online platforms

Future outcome 5.3: Consumers will be less vulnerable to fraud via telecommunications channels such as telephone texts and SMS messages

Future outcome 5.4: Technology, financial services and telecommunications sectors and their respective regulators will cooperate more closely on combatting payment fraud.

Future outcome 5.5: Greater awareness of fraud and fraud prevention among Irish consumers.

Future outcome 5.6: Consumers will be more aware of the risk of payment fraud including that committed via telecommunications, financial services and/or online platforms.

Account-to-account payments

Future outcome 6.1: Availability of at least one 'pay by account' solution as a convenient and trusted alternative to cards and cash.

Future outcome 6.2: Greater awareness of open banking and account-to-account services among Irish payment service providers.

The future of payments

Future outcome 7.1: Stakeholders will have greater awareness of best practices and areas of opportunity across the payment ecosystem in the area of sustainability.

Data collection, analysis and sharing

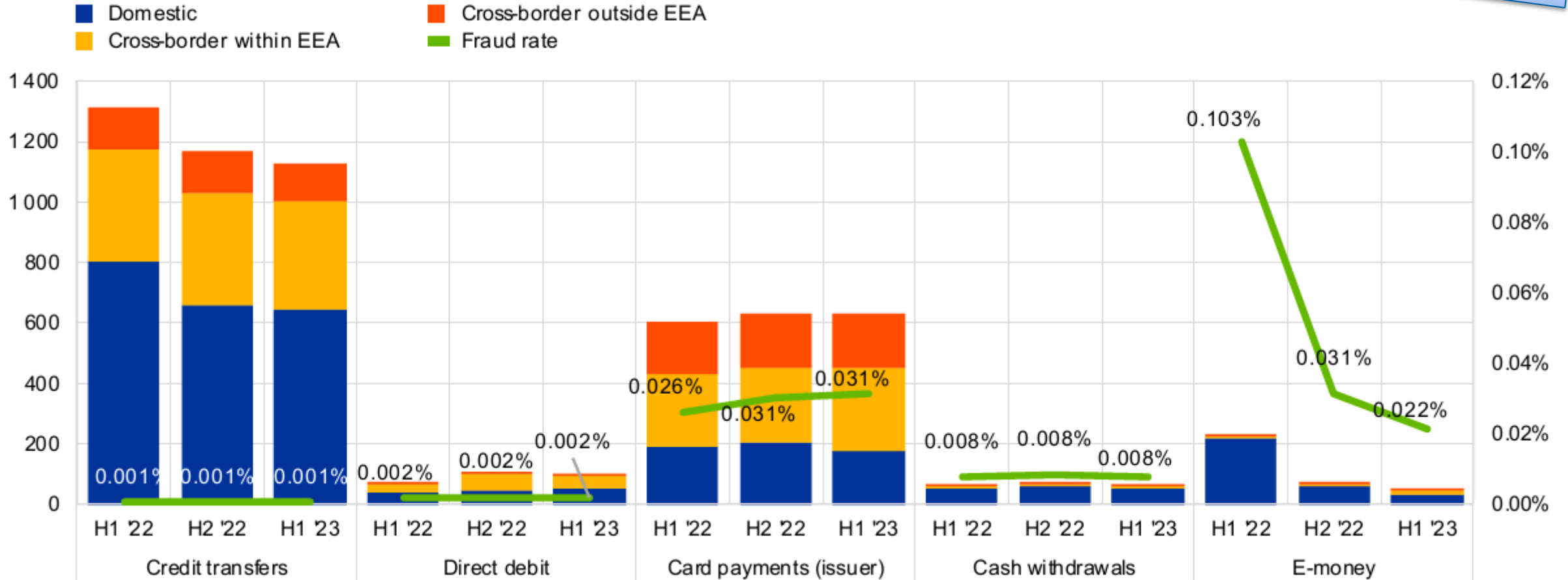
Future outcome 8.1: There will be greater transparency and understanding of the Irish payments landscape with insights on trends and usage of payment types.

Gemeinsamer Bericht von EZB und EBA zum Betrug im Zahlungsverkehr

Betrug nach Zahlungsinstrumenten

Absoluter und relativer Betrag nach Zahlungsinstrumenten (in Werten)

ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf



Profitcard- Betrug im Massenzahlungsverkehr

22. Januar 2025

Seite 4

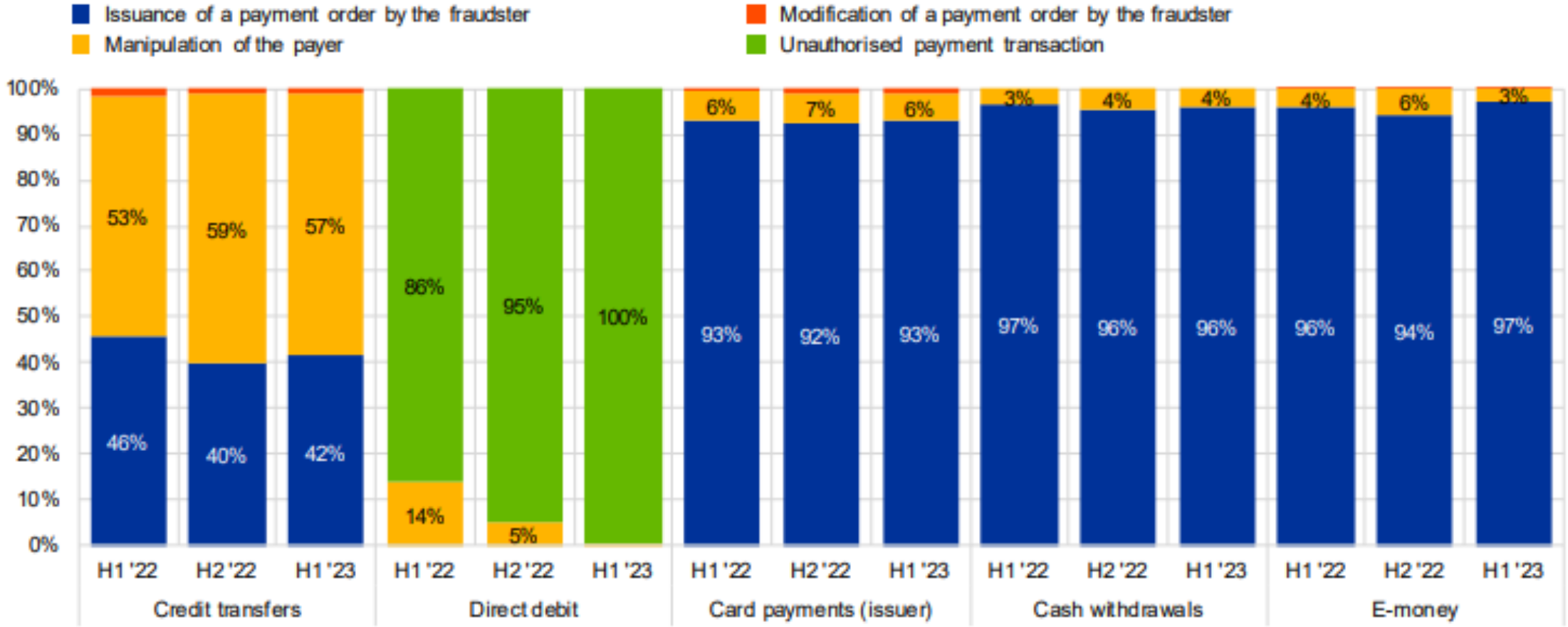
Linke Achse: Gesamter Betrag (Million EUR)
Rechte Achse: Betrag in Relation zum Gesamtwert der korrespondierenden Transaktionen

Gemeinsamer Bericht von EZB und EBA zum Betrug im Zahlungsverkehr

Wesentliche Betrugsarten

ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf

Betrug nach Haupt-Betrugsarten



Wert betrügerischer Transaktionen in Relation zum Gesamtwert des korrespondierenden Betrugs

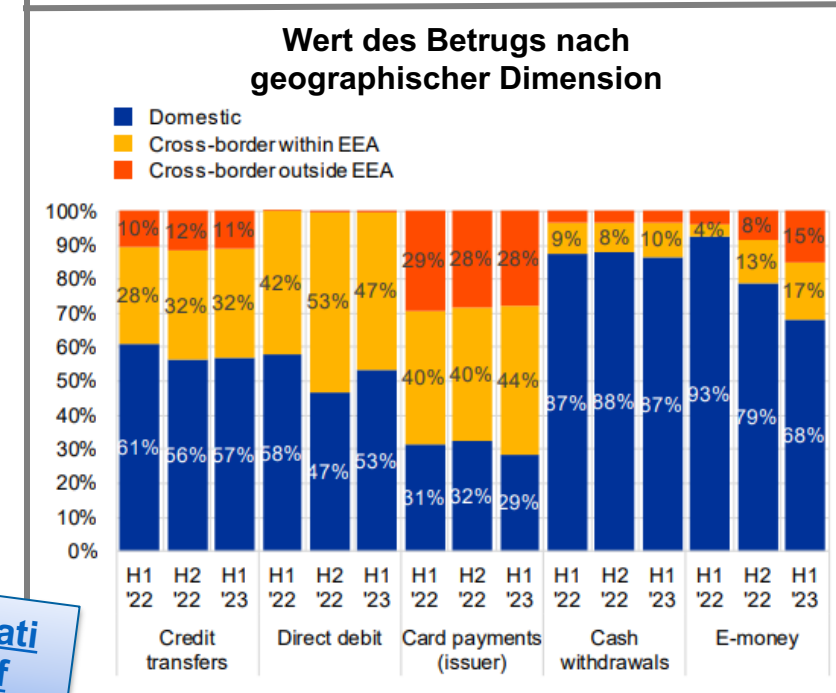
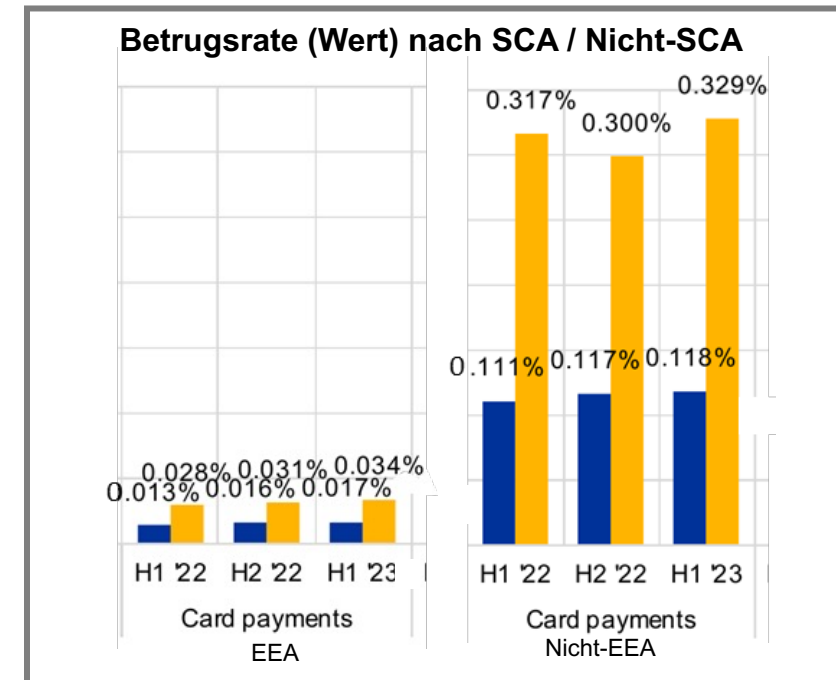
– **Positiver Einfluss der Starken Kundenauthentifizierung**

- Genutzt bei ca. 70% der Überweisungen und knapp 40% aller Kartenzahlungen
- Kartenbetrug innerhalb des EWR wesentlich geringer als bei one-leg out payments

– Die **Verteilung der Verluste** auf die Beteiligten (KundInnen, Dienstleister, Sonstige) divergiert relativ stark zwischen ZV-Instrumenten und Ländern (EWR)

- Bei Überweisungen tragen die KundInnen in H1 '23 den größten Anteil des Betrugs, es folgen Lastschriften und Kartenzahlungen
- In einigen Ländern tragen KundInnen einen Großteil des Betrugs, in anderen Ländern nur einen relativ geringen Teil

– Größter Teil des Kartenbetrugs und ein großer Teil des Betrugs bei Überweisungen und Lastschriften entfällt auf **grenzüberschreitende Zahlungen**



ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf

Manipulation

- Auslösung von Zahlungen
- Preisgabe von Informationen

Schub im Social Engineering



Malware

Verstärkt in Kombination mit Social Engineering

Bekannte Methoden

Phishing / Smishing / Vishing
Spoofing

Jeder kann Opfer von Betrug werden...

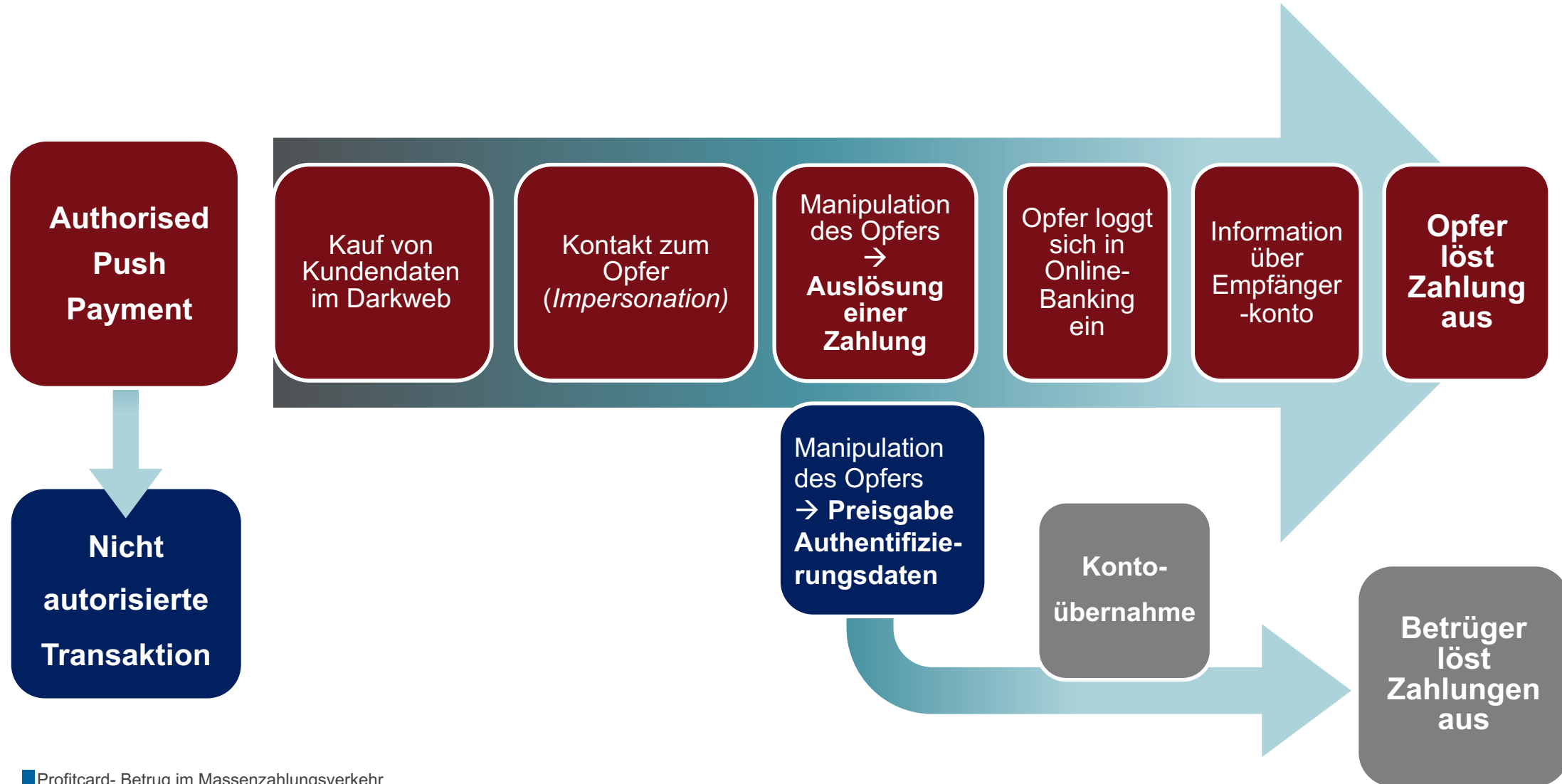
...unabhängig von Alter und Bildung



Ausgefeiltere Muster

- Sehr flexible Attacken
- Kombination von Betrugsarten
- Psychologische Techniken



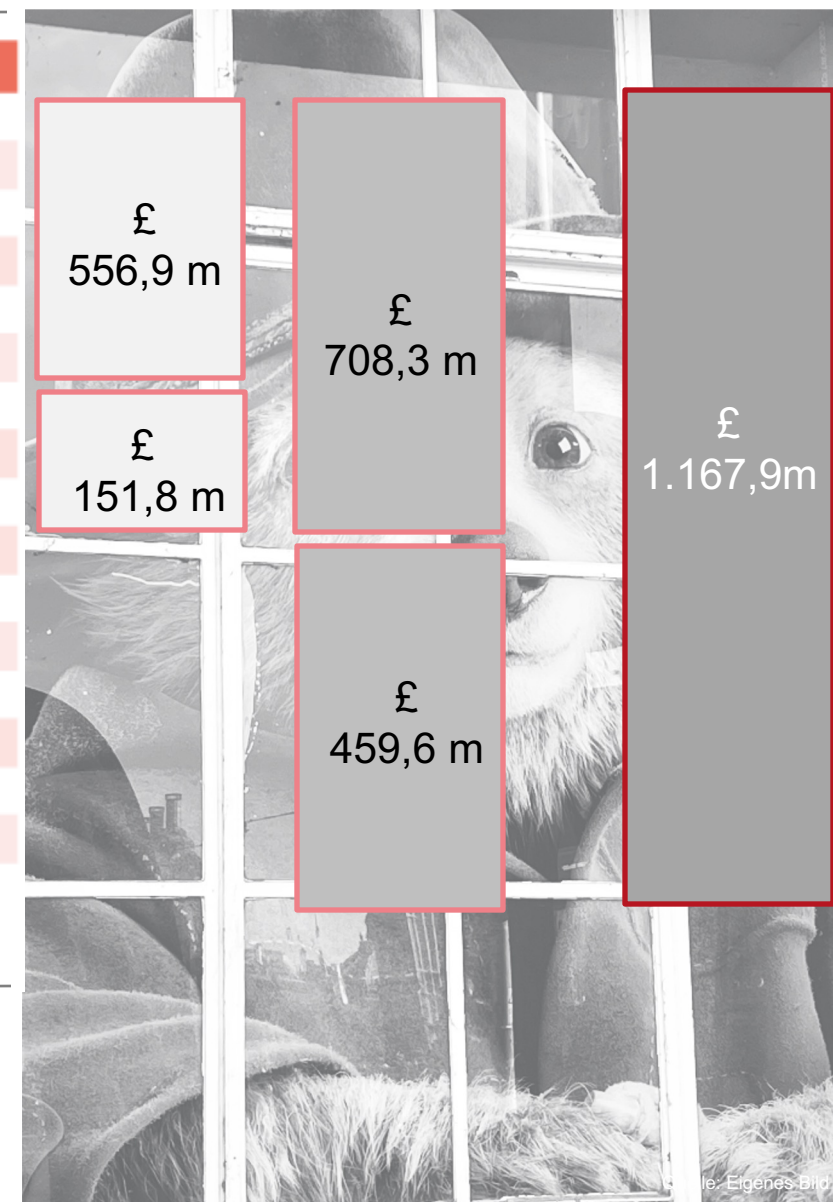


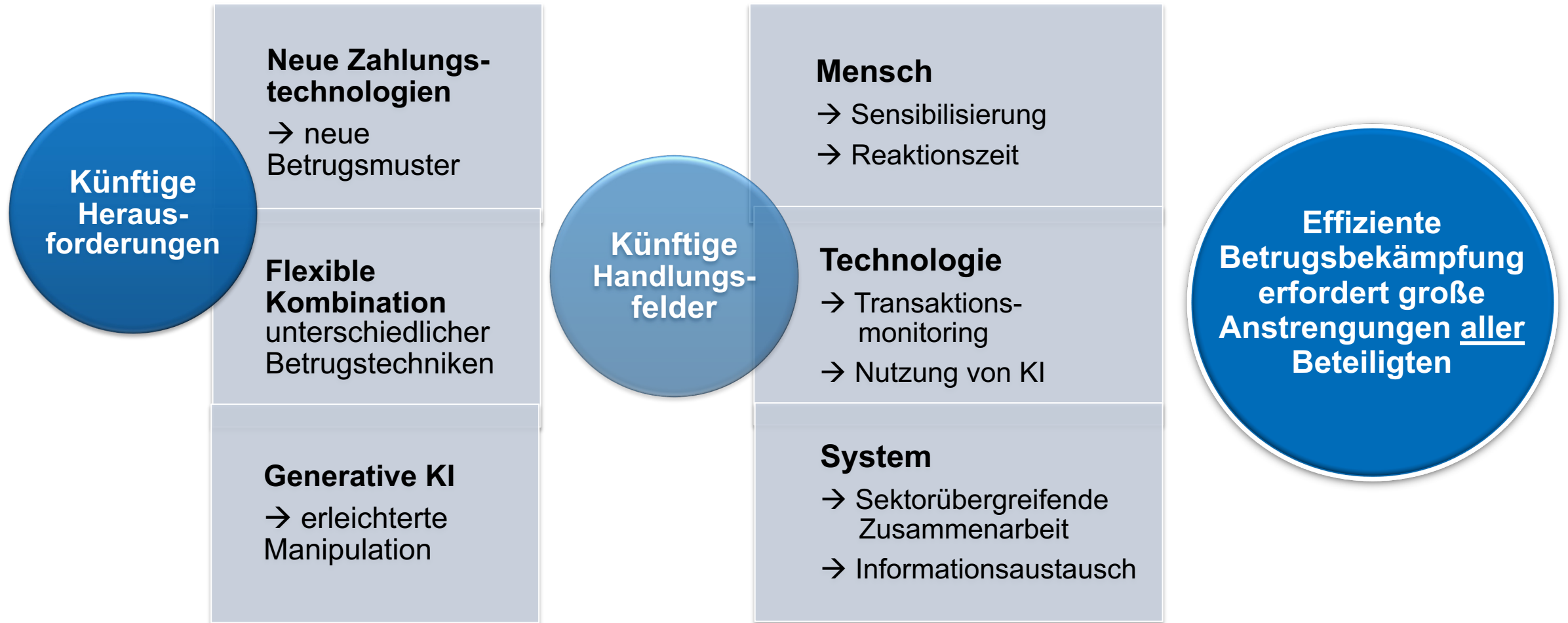
Secure Pay Forum - Task Force zur Analyse neuer Betrugsmuster

Entwicklungen am Beispiel UK

TYPE	CATEGORY	SUB CATEGORY	2020	2021	2022	2023	CHANGE
UNAUTHORISED	CARD	Lost & stolen	£78.9m	£77.2m	£100.2m	£104.0m	4%
UNAUTHORISED	CARD	CNR	£4.4m	£3.9m	£4.0m	£3.0m	-24%
UNAUTHORISED	CARD	Counterfeit	£8.7m	£4.7m	£4.7m	£4.7m	0%
UNAUTHORISED	CARD	Remote purchase	£452.6m	£412.5m	£395.7m	£360.5m	-9%
UNAUTHORISED	CARD	Card ID Theft	£29.7m	£26.3m	£51.7m	£79.1m	53%
UNAUTHORISED	CHEQUE	Cheque	£12.3m	£6.4m	£7.5m	£5.6m	-25%
UNAUTHORISED	REMOTE BANKING	Internet Banking	£159.7m	£158.3m	£114.1m	£88.7m	-22%
UNAUTHORISED	REMOTE BANKING	Telephone Banking	£16.1m	£15.5m	£14.7m	£17.6m	19%
UNAUTHORISED	REMOTE BANKING	Mobile Banking	£21.6m	£25.8m	£34.2m	£45.5m	33%
AUTHORISED	PAYMENT	Invoice & Mandate scam	£68.8m	£56.7m	£49.5m	£50.3m	2%
AUTHORISED	PAYMENT	CEO scam	£4.8m	£12.7m	£13.4m	£11.6m	-14%
AUTHORISED	PAYMENT	Impersonation: Police/Bank	£90.9m	£137.3m	£109.8m	£78.9m	-28%
AUTHORISED	PAYMENT	Impersonation: Other	£55.8m	£77.5m	£67.8m	£57.3m	-16%
AUTHORISED	PAYMENT	Purchase scam	£51.1m	£64.1m	£67.0m	£85.9m	28%
AUTHORISED	PAYMENT	Investment scam	£109.4m	£171.7m	£114.1m	£107.8m	-5%
AUTHORISED	PAYMENT	Romance scam	£17.8m	£30.9m	£31.3m	£36.5m	17%
AUTHORISED	PAYMENT	Advance Fee scam	£22.2m	£32.1m	£32.2m	£31.3m	-3%

Quelle: UK Finance, Annual Fraud Report 2023





Secure Pay Forum - Task Force zur Analyse neuer Betrugsmuster Echtzeitüberweisungen und Betrug

Key Features*	Fraud Considerations
Posting speed	<ul style="list-style-type: none"> • Strict service-level agreements based on scheme rules mean that payment service providers and FPS operators have little time to run fraud checks (such as anti-money-laundering or countering the financing of terrorism). • Even if fraud is identified, the time to respond is much shorter because the recipient has immediate access to funds and can move them between many accounts (that is, so-called money mules).
24/7/365 availability	<ul style="list-style-type: none"> • Fraudsters can work around the clock and at odd hours, especially when bank staff members are not active. For this reason, victims may not be able to check their accounts and report fraudulent activity to the authorities quickly.
Payment finality	<ul style="list-style-type: none"> • Money that is fraudulently stolen from an account cannot be easily reversed, as with a card payment (for example, chargebacks). • By the time a transaction is deemed to have been fraudulent, the illegally obtained funds may already be gone. This can make lost funds very hard to recover.
High transaction limits	<ul style="list-style-type: none"> • The ability to send a large amount of money in a single transaction can make fast payments very attractive for fraudsters.

* nicht abschließend

Quelle: World Bank, Fraud in Fast Payments (2023)

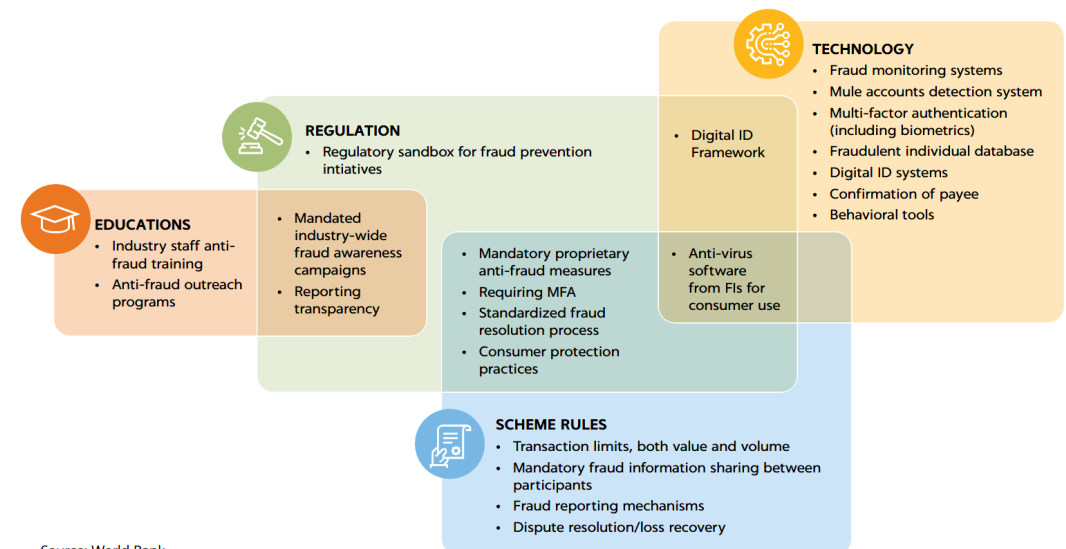
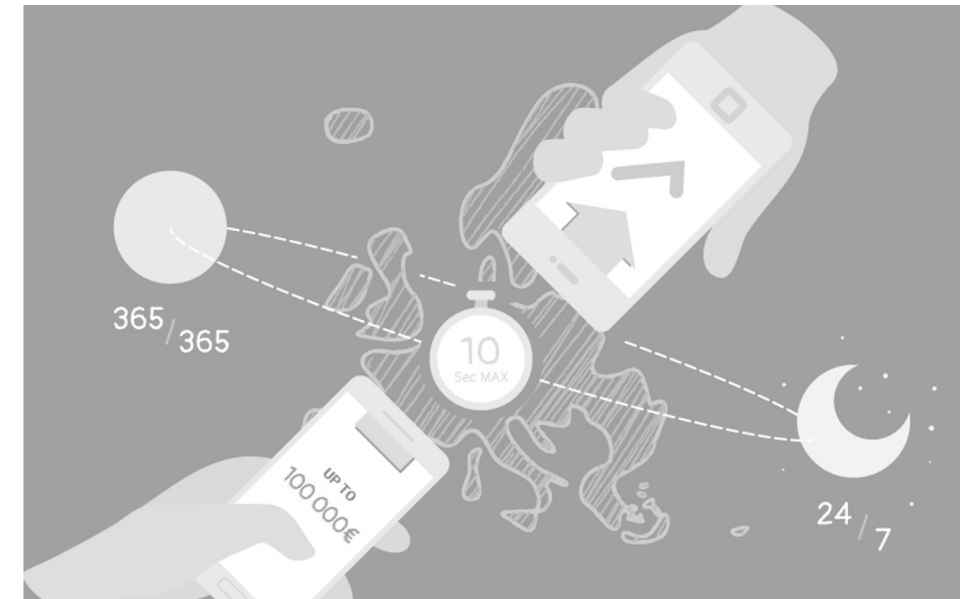
Profitcard- Betrug im Massenzahlungsverkehr

22. Januar 2025

Seite 11

The first is instant credit transfers, also referred to as instant payments, for which the data reported by 18 NCAs for H1 2022, show that the fraud rates in value, besides presenting significant divergences between Member States (MS), **are about 10 times higher on average** than conventional Credit Transfers (CT).

Quelle: EBA, Opinion on new types of payment fraud (2024)



Source: World Bank

Veröffentlichung im September 2024

Fokus auf Betrugsprävention und -mitigation basierend auf vier *gamechangern*

1. Sektorübergreifende Zusammenarbeit und Verantwortlichkeit von Marktteilnehmern

- Errichtung eines EU-Netzwerks unter Koordination des EPC
- Stärkung bereits bestehender Kooperationen

2. Austausch von Erfahrungen zu Betrugsmustern und von relevanten Daten

- Errichtung eines EU-weiten “Netzwerks von Netzwerken” zum Austausch von Betrugsdaten
- Erkundung von Möglichkeiten für einen schnellen Informationsaustausch (z.B. mit Strafverfolgungsbehörden, Internetplattform- und Telefonnetzbetreibern)

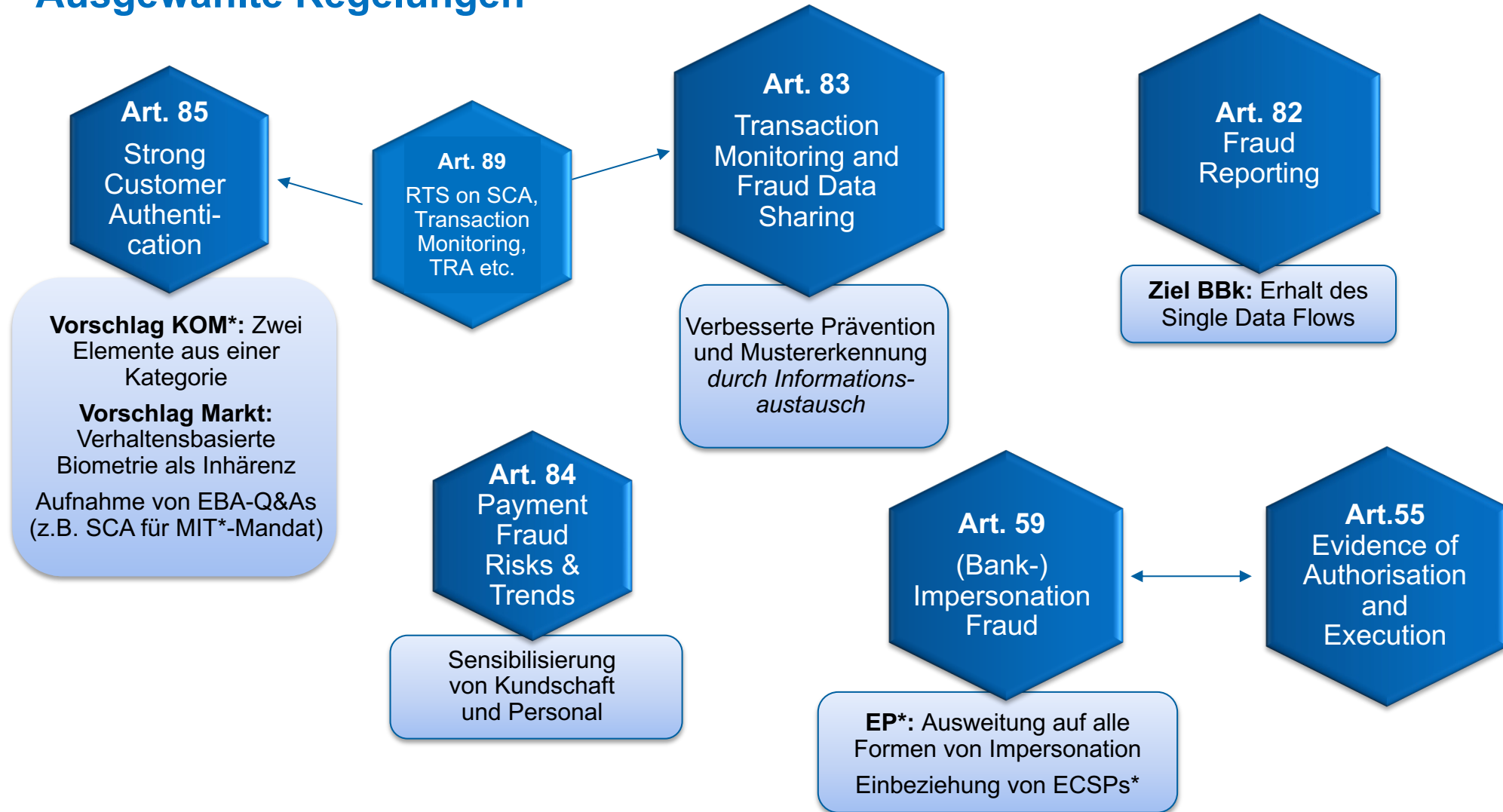
3. Sektorübergreifende Zusammenarbeit von EU-Aufsichtsbehörden

4. Sicheres Produktdesign zum Schutz von VerbraucherInnen

Ideensammlung ohne Bewertung
der Wirksamkeit der einzelnen
Maßnahmen

- **Sensibilisierung** von MitarbeiterInnen, VerbraucherInnen und HändlerInnen für potentielle Risiken
- Nutzung von **Machine Learning** und KI-basierten **Prognosemodellen**
- **Austausch** von **Informationen** über aktuelle Betrugsformen und von **Daten** zu realen Betrugsfällen
- **Sektorübergreifende Regulierung** (Einbeziehung von Internetplattform- und Telefonnetzanbietern)
- **Szenariobezogene Maßnahmen zur Reduzierung von Risiken**
 - Nutzung von Starker Kundenauthentifizierung / EMV 3DS für CNP-Käufe
 - Einführung / Anpassung von Regeln und Restriktion an Nutzerverhalten, Produktkategorien, Zahlungsbetrag, Kaufsituation etc. (z.B. Limits, (De-)aktivierung Kontaktloszahlung, Versand von Warnhinweisen und Benachrichtigungen)
 - Einfache Sperrmöglichkeit für Zahlungsmittel
 - Verifikation der ZahlungsempfängerInnen

Ausblick PSR – Ausgewählte Regelungen



- **ECSP:** Electronic Communication Service Provider
- **EP:** Europäisches Parlament
- **KOM:** Europäische Kommission
- **MIT:** Merchant Initiated Transactions



Dirk Schrade
Ständiger Vertreter des Leiters des Zentralbereichs
Zahlungsverkehr und Abwicklungssysteme

Zentrale
Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main
Telefon: +49 69 9566-34315, Telefax: +49 69 956650-8046
dirk.schrade@bundesbank.de



Profitcard- Betrug im Massenzahlungsverkehr

22. Januar 2025

Seite 15