Bundesministerium
Inneres

Bundeskriminalamt

bundeskriminalamt.at

# GW/TF – Webinar WKO Unternehmensberater:innen

## „Geldwäsche aus kriminalistischer Perspektive“

Mag. Mathias BERGER

Bundeskriminalamt
7.3 – Zentrale Geldwäschemeldestelle
Austrian Financial Intelligence Unit (A-FIU)

# Wen stellen Sie sich unter einem Geldwäscher vor?


Die Optik verrät den Geldwäscher nie. Es geht um das Gesamtverhalten!

# Dimension der Geldwäsche

**laut United Nations Office on Drugs and Crime (UNODC)**

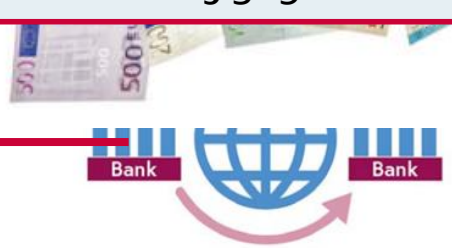
- 80 % der Straftaten finanziell motiviert
- Reduzierung der globalen Wirtschaftsleistung/Jahr um ca. 5 %
- Ca. 2 Billionen Euro kriminelle Gelder werden im Jahr gewaschen
- Langfristiger und nachhaltiger Wachstumsverhinderer der Wirtschaft

# Geldwäsche und wie diese abläuft

Gegenstände werd
zum Händler gebra
– gegen Bargeld
getauscht ?

**Zur Prävention gibt es die Sorgfaltspflichten nach §§ 365p ff GewO**
KYC-Check, Mittelherkunftsprüfung
Risikobewertung essentiell (konkretes Risiko der Gewerbetreibenden; dazu goAML-Registrierung)
§ 365n1 GewO

iminelle Handlung:
. Falscher
lizistentrick

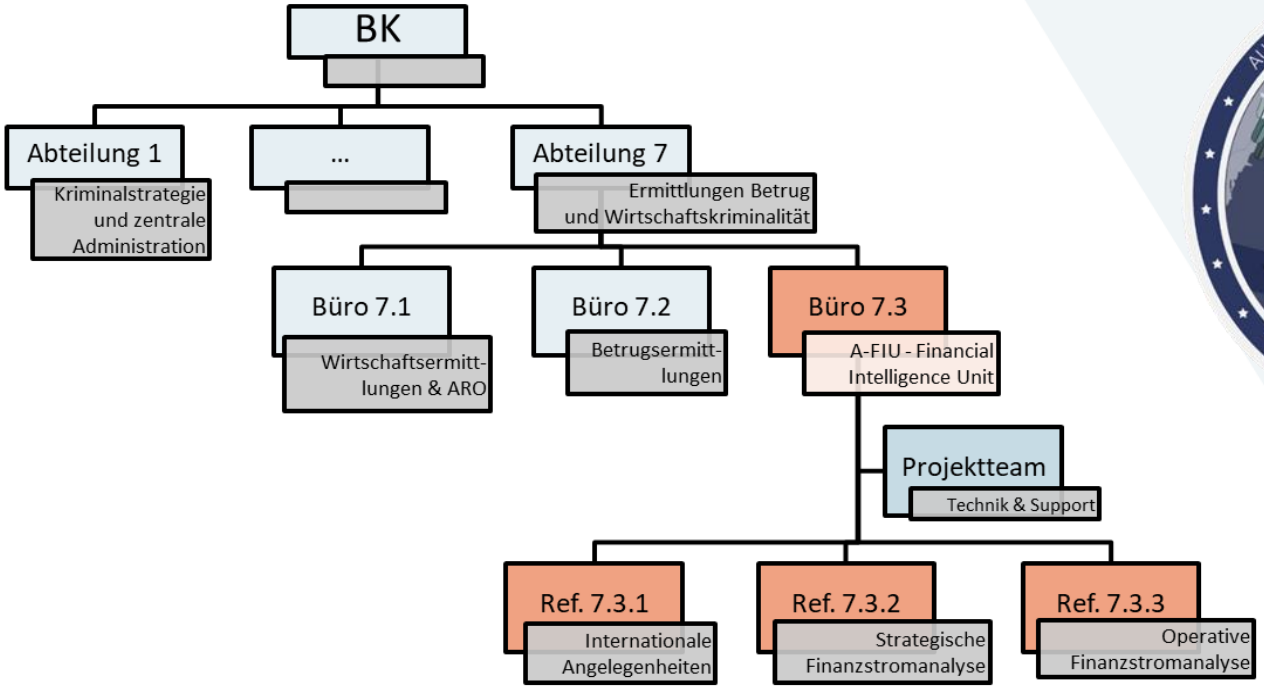



Verschleierung des Ursprungs des Geldes durch kreative Wege – häufiges Hin- und Her transferieren (auch ins Ausland) …

aschenes Geld wird wieder angelegt – Immobilien oder Luxusgüter

# Die A-FIU und die GW/TF-Prävention

# Die A-FIU / Zentrale Geldwäsche-Meldestelle



# Geldwäschemeldestelle

Büro 7.3.3

- Kontakt: 1090 Wien, Josef Holaubek Platz 1

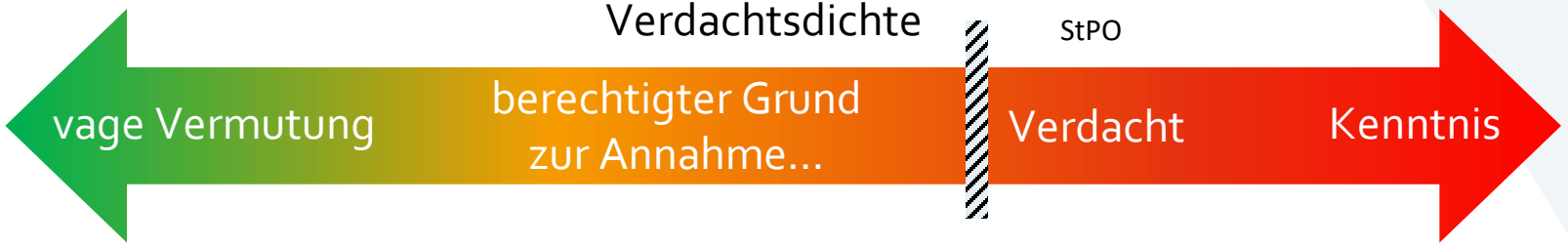
  Tel.: +43 1 24836 985298 → **Geldwäschemeldestelle/A-FIU**

  E-Mail: a-fiu@bmi.gv.at

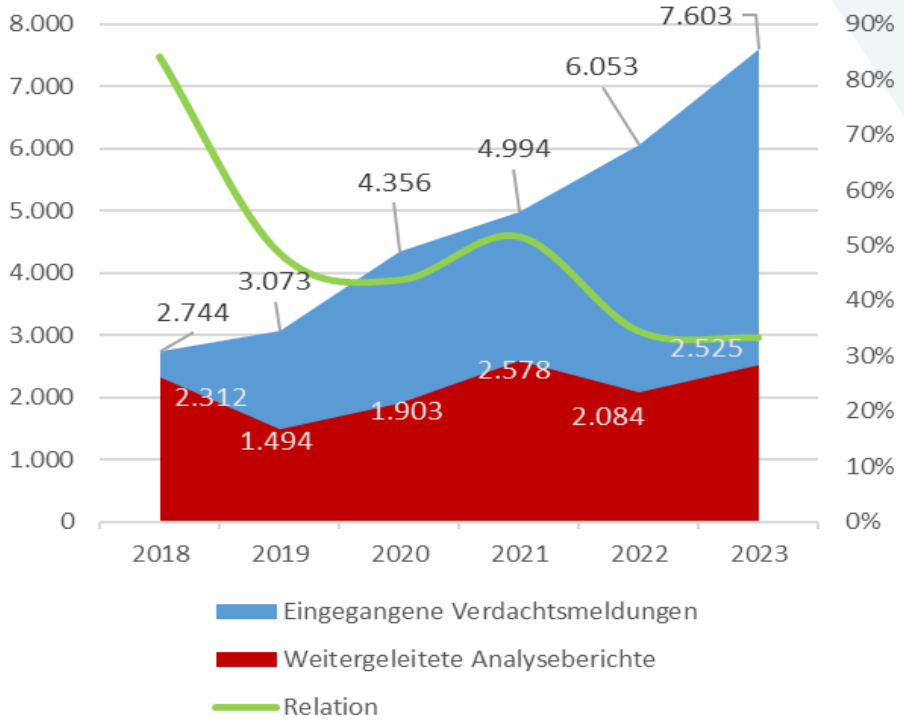
- Journal: **Geldwäschemeldestelle/A-FIU** von Montag bis Freitag (werkt.) von 09:00 Uhr bis 17:00 Uhr

# Meldepflicht gegenüber der A-FIU

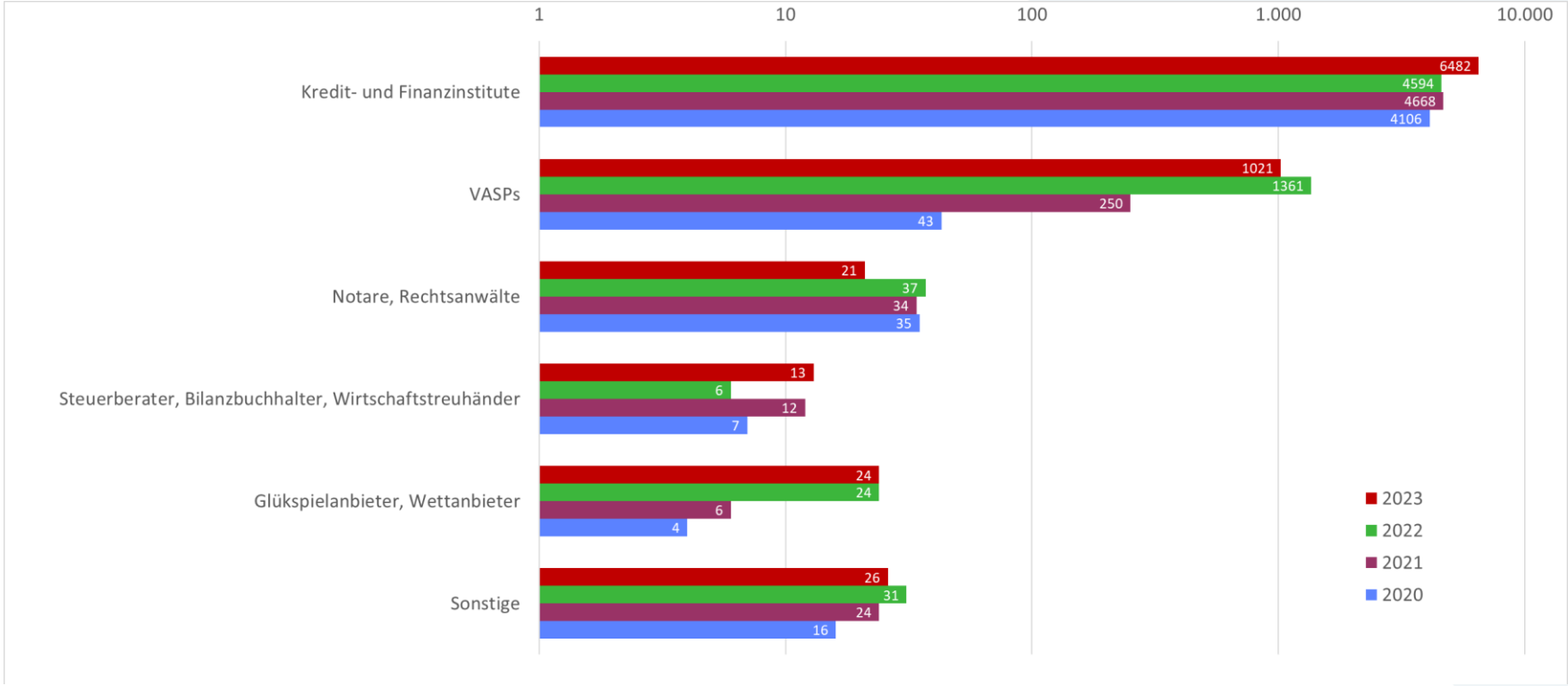
- Erstattung einer Verdachtsmeldung verpflichtend, wenn
  - Verdacht oder
  - berechtigter Grund zur Annahme,
- dass Transaktion/Geschäft in Zusammenhang mit Geldwäscherei oder Terrorismusfinanzierung steht



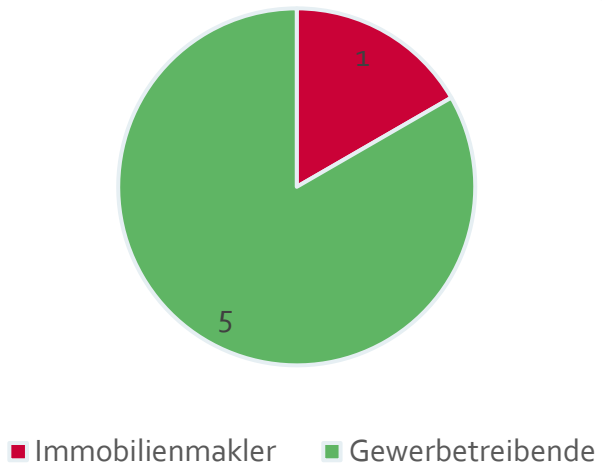
# Filterfunktion



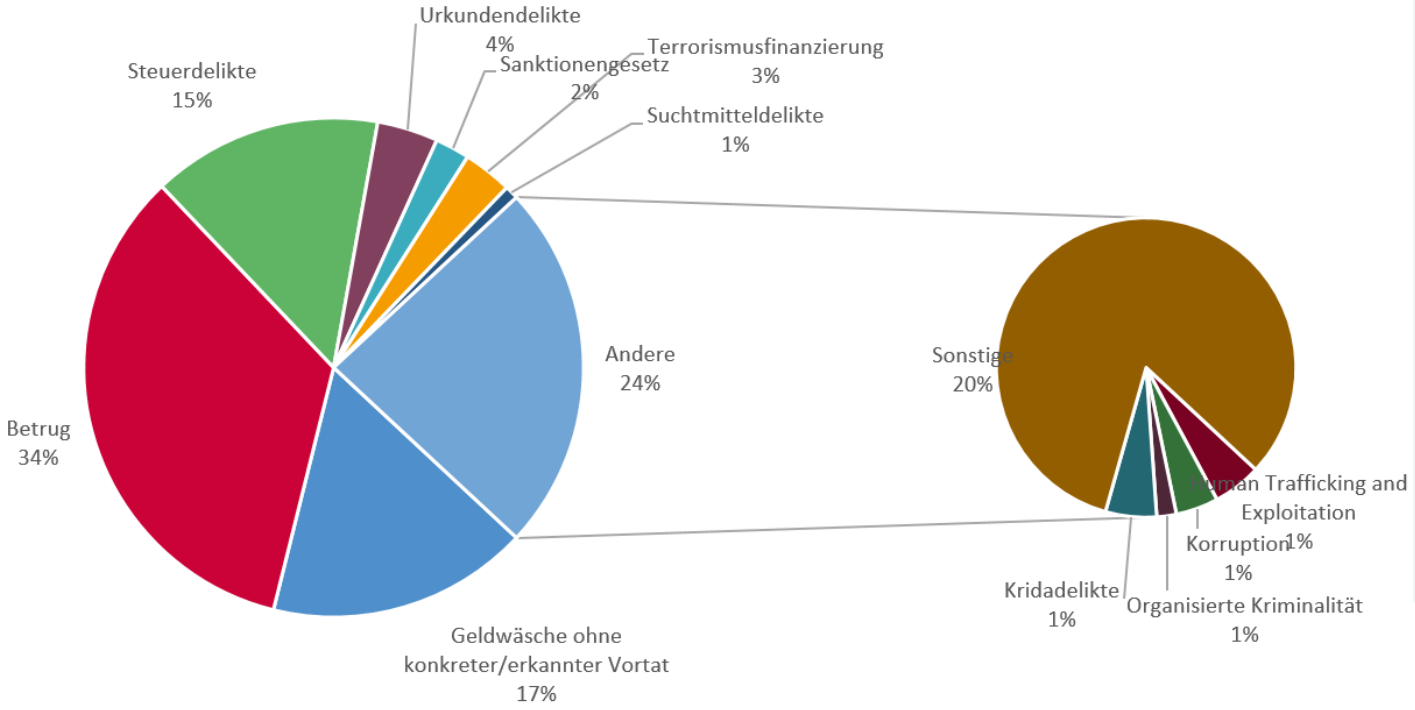
# Verdachtsmeldungen nach Berufsgruppen



# Verdachtsmeldungen Gewerbe 2023



# Anteil der Deliktsbereiche



# Meldepflichtige Berufsgruppen

- Risikobehaftete Berufsgruppen
- Sektoren, die anfällig für geldwäschegeeignete Geschäfte sind, wie etwa Banken, ImmobilienmaklerInnen, RechtsanwältInnen, NotarInnen, Gewerbetreibende (**Unternehmensberater**), Glücksspielunternehmen, Versicherungsvermittler etc.
- Unternehmensberater fallen nur für bestimmte Tätigkeiten unter die GW/TF Bestimmungen:
    - Gründungen, Bestimmte Funktion, Bereitstellung Sitz etc, Treuhänder oder ähnliches, Ausübung Funktion eines nominellen Anteilseigners für andere Person

# Risikobasierter Ansatz

- Im Kampf gegen GW/TF unerlässlich
- Element Gewerbe: **Risikoerhebungsbogen** – Feststellung des konkreten Risikos sehr wichtig!
- Es geht um das: **konkrete Risiko** des Gewerbetreibenden
  - Je nach Kundenstock,
  - Branche/Verkaufsgegenstände unterschiedlich
  - zB Immobilienmakler Kitzbühel anderes Risiko als Goldhändler in Wien
  - Wichtiger Baustein im Kampf gegen GW/TF – Risikobeurteilung!

# Strategische Entwicklungen in der FIU

# Neues Mitteilungssystem der A-FIU

## Red Notice

- Warnmitteilung zu konkreten, aktuellen Modi Operandi
- rasches Handeln erforderlich
- Übermittlung via goAML Inbox/E-Mail

## Purple Notice

- Phänomene, Trends & Muster
- Übermittlung via goAML Homepage

## Green Notice

- Neuigkeiten aus der A-FIU
- Entwicklungen & Zwischenstände
- Erfolgsmeldungen
- Übermittlung via goAML Homepage

# goAML Registrierungen

- A-FIU darf Kommunikationskanal festlegen (§ 365t Abs. 1 Z3 GewO): goAML
- Ausgangslage bei Registrierungen (Stand Oktober 2024):
  - Ca. 1.800 Registrierungen des Gewerbesektors in Österreich
- Warum ist das wichtig und welche Vorteile haben Sie von einer Registrierung?
  - FATF Prüfung
  - Informationen von der A-FIU empfangen – Risikobewertung (§ 365 n1 GewO)
    - ➢ Selbstschutz vor Missbrauch
  - Unverzügliche Abgabe einer Verdachtsmeldung
  - Umgehung einer möglicher Strafe der Aufsicht

# Leitfaden Gewerbetreibende

- Auf Homepage Bundeskriminalamt veröffentlicht
  - Februar 2024
- Hinweise zu goAML
- Anleitung Registrierung
- Indikatoren
- Überblicksmäßig und vereinfacht dargestellt – Rechtslage
  - Nicht nach Bereiche spezifiziert

# Online-Kontoeröffnungen mittels gefälschter Ausweise

- Tätergruppe eröffnet mit gefälschten Ausweisen Konten
  - entweder durch Online-Verifizierungen oder durch 1 Cent-Legitimationen
- Besonderheiten:
  - Personendaten der Ausweise sind reellen, unbeteiligten Personen zuzuordnen -> Identitätsdiebstahl
  - Verwendete Adressen oftmals Arztpraxen, Geschäftslokale etc.
  - Österreichische Reisepässe sowie Dienstpässe (Mix aus Daten)

# Online-Kontoeröffnungen mittels gefälschter Ausweise

- Bisher 10 gefälschte Identitäten einer Tätergruppe festgestellt
- Bisher 38 Konten (alle per Online-Verifizierungsverfahren und 1 Cent Legitimation eröffnet) identifiziert
- Drei Banken waren betroffen – 21 Konten bei einer Bank
- Konten wurden genutzt, um weitere Konten zu eröffnen, Gelder aus Betrugshandlungen zu erhalten und weitertransferieren bzw. abzuheben
- Teilweise hatte die echte Identität auch bereits Konten bei den Banken

# Online-Kontoeröffnungen mittels gefälschter Ausweise

- Red Notices der A-FIU vom 11.03. und 20.03.2024
- Purple Notice vom 22.03.2024 zum Phänomen an sich
- A-FIU gem. § 16 Abs. 6 FM-GwG zum Austausch
  - von Dokumenten,
  - Informationen sowie
  - Kundendaten

zum Zwecke der Bekämpfung von GW oder TF ermächtigt.


RED NOTICE

Warnmitteilung

Diese Warnmitteilung ist ein Update zur Warnmitteilung der A-FIU vom 11.03.2024:

Update: Kontoeröffnungen mittels gefälschter Ausweise

Wie bereits informiert, eröffnet derzeit eine unbekannte Tätergruppe in Österreich Konten mittels Online-Verifizierungen bzw. SEPA-Verifizierungen (1-Cent).

Die bei der Verifizierung genutzten Ausweiskopien enthielten in allen Fällen deutlich erkennbare Musiknoten/Notenschlüssel. Der österreichische Reisepass enthält dieses Sicherheitsmerkmal zwar tatsächlich, die Musiknoten/Notenschlüssel sind auf authentischen Scans/Fotos aber weniger gut sichtbar und nicht so stark ausgeprägt wie auf den derzeit verwendeten Totalfälschungen.

Des Weiteren ist auf den gefälschten Dokumenten seitlich die DVR Nr. gedruckt, die auf legitimen Dokumenten seit 25.05.2018 nicht mehr gedruckt wird.

Fälschung

20.03.2024 BMI II / BK / 7.3 (A-FIU) 1

admin Log out

VERIF TOOLS

USA Passport

Balance: 50.00 $ Top up

All Generators

- USA Passport
- Germany Passport
- Lietuva Passport

Step 1 | Step 2 | Step 3 | Step4

Input fields

Surname
Housten

Given Names
Jacob

Document Number
963545023

Sex
M

Result:


Download

# Online-Kontoeröffnungen mittels gefälschter Ausweise



Kopien/vermeintliche Scans werden auch gerne bei Händlern verwendet

# Online-Kontoeröffnungen mittels gefälschter Ausweise

RED NOTICE

## Warnmitteilung

**Die Warnmitteilung der A-FIU vom 11.03.2024:**

### Kontoeröffnungen mittels gefälschter Ausweise

Eine derzeit unbekannte Tätergruppe eröffnet mit gefälschten Ausweisen und mittels durch Identitätsdiebstahl erlangte Daten per Online-Verifizierungen sowie durch 1 Cent Legitimationen Konten in Österreich und dies in kurzer zeitlicher Abfolge (lt. Kontenregisterauswertung mehrere Konten an einem Tag eröffnet). Diese Konten werden verwendet um inkriminierte Gelder aus Betrugshandlungen von bisher ausschließlich ausländischen Opfern (besonders deutsche Opfer) zu empfangen und weiterzuleiten.

**Achtung: Die Personendaten der Ausweise sind reellen, mutmaßlich unbeteiligten Personen zuzuordnen. Diese Personen sind mit hoher Wahrscheinlichkeit Opfer eines Identitätsdiebstahls geworden.**

Die Vorgangsweise der Täterschaft ist, dass Daten von echten Personen mit gefälschten Fotos und zum Teil abgeänderten Passnummern genutzt werden. Teilweise werden Dienstpassvorlagen verwendet, wobei die Passnummer auf „U" statt „P" geändert wird. In einigen Fällen werden Passnummern und Personendaten von reellen Personen vermischt und in falschen Reisepässen zusammengefügt.

Sehr auffällig ist die verwendete Unterschrift, die eine handschriftliche Schriftart (ev. Word-Vorlage) zu sein scheint und bisher in allen Fällen gleich aussieht. Ebenso ergeben sich bei der letzten Kontrollzeile Ungereimtheiten bspw. beim Geburtsdatum und auch das verwendete Bild ist im Verhältnis zu anderen Reisepässen als zu groß einzustufen bzw. passt das angeführte Alter teilweise nicht zum verwendeten Foto.

Die zu den Kontoeröffnungen verwendeten Adressen wurden auffällig, da diese oftmals keine für Wohnzwecke geeignete Adressen sind bspw. Arztpraxen oder sonstige Auffälligkeiten beinhalten, die mit einer simplen OSINT-Recherche gefunden werden können. Jedoch wurden auch Adressen der echten Identität zur Eröffnung genutzt.

Wie die Täter an die persönlichen Informationen und Reisepässe der Opfer gelangt sind, kann bisher nicht abschließend geklärt werden.

Folgende Ausweise bzw. Falschidentitäten sind bisher bekannt, da nicht auszuschließen ist, dass diese Fotos auch mit anderen Falschidentitäten verknüpft und verwendet wurden, ersuchen wir auch um Kontrolle abseits der bisher bekannten Alias-Namen mit den verwendeten Fotos:



PURPLE NOTICE

## Phänomene, Trends & Muster

### Online-Identifikation

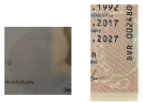
Für die Zwecke der Identifikation der Kunden (§ 6 Abs. 1 Z 1 FM-GwG) bedienen sich betroffene Verpflichtete verschiedener Anbieter für Online-Identifikation. Unter Berufung auf eine der alternativen Identifikationsmethoden gemäß § 6 Abs. 4 FM-GwG unterbleibt ein persönlicher Kontakt mit den Kunden und es kommt auch zu keiner persönlichen Vorlage eines amtlichen Lichtbildausweises.

Mit diesen alternativen Identifikationsmethoden sind erhöhte Missbrauchsrisiken verbunden, die das FM-GwG durch die verpflichtende Anwendung kompensierender Sicherheitsmaßnahmen einschränkt. Die vielen Beispiele von totalgefälschten Identitätsdokumenten, mit denen eine „Identität" erfolgreich bestätigt und im Anschluss eine Geschäftsbeziehung eröffnet wurde, zeigen jedoch deutlich, dass die gesetzlich vorgesehenen Sicherungsmaßnahmen im Zuge der Online-Identifikation vielfach nicht in ausreichendem Maße erfüllt werden.

Als Beispiele für die mangelnde Qualität bei der „Identifizierung" von potenziellen Kunden sind – den verfahrensbezogenen Sicherungsmaßnahmen der Online-Identifikationsverordnung – Online-IDV folgend – anzuführen:

*Visuelle Überprüfung des Vorhandenseins der optischen Sicherheitsmerkmale einschließlich bewegungsoptischer (holographischer) oder gleichwertiger Sicherheitsmerkmale, die nach Aufforderung zum horizontalen und vertikalen Kippen des amtlichen Lichtbildausweises deutlich erkennbar sein müssen (§ 4 Abs. 4 Z 1 Online-IDV)*

Die allermeisten der festgestellten Totalfälschungen enthalten nicht einmal ansatzweise nachgemachte holografische oder gleichwertige Sicherheitsmerkmale, die durch Kippen der Ausweise in der Kamera erkannt werden könnten (oftmals nur weiße oder graue Drucke, die keine holografischen Fähigkeiten haben). Die A-FIU geht davon aus, dass vielfach überhaupt keine Videoprüfung stattfindet, sondern eine Fotoprüfung, bei der bewegungsoptische Sicherheitsmerkmale überhaupt nicht betrachtet werden können. Ein Umstand der ohne Videoprüfung ohnehin nur schwer feststellbar ist.



# Online-Kontoeröffnungen mittels gefälschter Ausweise

- Identitätsdiebstahl kann zu massiven Problemstellungen führen:

**Rechtsverkehr:**

- Eröffnete Konten als Legitimation für weitere Kontenöffnungen
- Reputations- und Imageschäden
- Finanzielle Schäden für Bankinstitute

**Persönlicher Natur:**

- Strafrechtliche Konsequenzen
- Finanzielle Schäden
- Eintragungen in Schuldnerregistern

Bundesministerium
Inneres

Bundeskriminalamt

# Hilfsmittel zur Dokumentenprüfung

## Überprüfung der maschinenlesbaren Zone


**Identifizierung des Kunden**

Augenschein von Dokumenten

Weblinks für Identitätsprüfungen:

**PRADO**:
https://www.consilium.europa.eu/prado/de/prado-start-page.html
Öffentliches Onlineregister echter Identitäts- und Reisedokumente für sämtliche EU-Mitgliedsstaaten sowie Island, Norwegen und Schweiz.

**IDENTT**:
https://www.identt.info/produkte/
Deutsche Datenbank für Ausweisdokumente, Banknoten und Online Identifizierung – Kostenpflichtig!

**World-Check:**
https://www.refinitiv.com/en/products/world-check-kyc-screening/world-check-one-kyc-verification
Kostenpflichtige Online Datenbank für PEP, Globale Sanktionslisten, negative Medien etc.

# Phänomen bei Gründungen 2024

- Vermehrtes Aufkommen von Unternehmensgründungen – überwiegend GmbHs
  - Gründer französische Staatsbürger
  - Sitz in Wien
  - Verwendung von gefälschten Ausweisen
  - Verwendung renommierter, prestigeträchtiger Adressen (Rechtsanwaltschkanzleien etc.)
  - Verwendung der Unternehmen für Betrugshandlungen im Ausland

# Sensibilisierung, Strafen & der Weg zu einer erfolgreichen GW/TF-Bekämpfung

- Sehr hoher Sensibilisierungsgrad im Finanzsektor
  - Resultat hoher Kontrollfrequenz FMA und spürbarer Strafaussprüche
- 100 %-Quote goAML-Registrierungen
- hohe Anzahl an Verdachtsmeldung
- gute Kooperation mit FIU
- Kontrollen auch im Gewerbebereich deutlich erhöht bzw. werden sich erhöhen

# Geld kann aus schwerwiegender Straftat (Vortat) stammen

- Immer vom Schlimmsten ausgehen – Was ist für Sie die schlimmste Vortat?
  - Generiertes Geld aufgrund von Kinderpornografie?
    - ➢ Auch hierzu bekommen wir Meldungen
  - Falscher Polizist?
    - ➢ War auch in Ihren Familien, Bekanntenkreis wer betroffen?
    - ➢ Immer wieder Bezug zu Gewerbetreibende (Gold, Juwelenhandel)

# Fall 1: Edelmetallhändler

- Ausgangslage
  - A-FIU erhielt Anfrage von ausländischer Partnerbehörde zu einer Transaktion über EUR 400.000,00 von einem österreichischen Konto auf das slowakische Konto der Frau B.

- A-FIU startete Analyse:
  - Datenbankabfragen und Anfragen an Banken durch die A-FIU
  - Sachverhalt konnte eruiert werden: Frau B. verkaufte 8 kg Goldbarren im Wert von EUR 400.000 bei Wiener Edelmetallhändler

# Fall 1: Edelmetallhändler

- Erlös von EUR 400.000,00 wurde auf slowakisches Konto überwiesen
- Der Edelmetallhändler wandte hierbei keine ausreichenden Sorgfaltspflichten an.
- Es wurde lediglich eine Unterschrift der Frau B. und die Bestätigung, dass Frau B. kein PEP sei eingeholt
- Kein ausreichender KYC Check
- Mittelherkunft hätte geprüft werden müssen!

Hier wäre ein Anwendungsfall der verstärkten Sorgfaltspflichten (§ 365s GewO) gegeben gewesen!

# Fall 1: Edelmetallhändler

- Vorgehensweise A-FIU:
  - Durchführung Analyse: Polizeiliche Datenbanken, Internat. Schriftverkehr
  - Weiterleitung des Analyseergebnisses in die Ermittlung
  - Sachverhaltsdarstellung an die MA63 zur aufsichtsbehördlichen Erledigung
    - Strafverfahren wurde eingeleitet
    - Aussage Unternehmer: Einzelfall, Kassiererin eigenmächtig gehandelt, sonst mache sie das natürlich nicht.

# Fall 2: Kauf von Liegenschaft durch Ukrainer

- Ausgangslage:
  - Ukrainischer Staatsbürger beabsichtigt Kauf von Liegenschaftsanteilen durch eine speziell gegründete Gesellschaft (Involvierung Unternehmensberater) in Salzburg, Wert EUR 3.500.000,00
  - Wr. Rechtsanwaltskanzlei setzt Kaufvertrag auf und ersucht eine **Bank O** um Eröffnung Treuhandkonto
  - Bank O **verweigert** die Durchführung des Geschäftes (aber keine Verdachtsmeldung an FIU)
  - Rechtsanwaltskanzlei wendet sich an **Bank N** und ersucht neuerlich um Einrichtung eines Treuhandkontos
    - Bank N **verweigert** die Durchführung des Geschäftes und erstattet Verdachtsmeldung

# Fall 2: Kauf von Liegenschaft durch Ukrainer

- A-FIU startet Analyse
  - Analyse deutet darauf hin, das Liegenschaftskauf auch der **Geldwäsche** dienen könnte, weil
    - Zahlreiche **Medienberichte**, dass ukrainischer Kaufinteressent von Ukraine wegen Veruntreuung und anderer Wirtschaftsdelikte gefahndet wird
    - **Ablehnung** durch Bank O und trotzdem Versuch über Bank N Geschäft abzuwickeln
    - **Insichgeschäft-Konstruktion**: Die Rechtsanwaltskanzlei und ihre Anwälte vertreten sowohl Käufer- als auch Verkäufer-Sphäre
    - **Mittelherkunftsnachweise** nicht geeignet, legale Herkunft der Gelder nachzuweisen (fehlende Unterschriften, fehlende Depot-auszüge oä).
    - **Komplexe Geldströme**, die Ukrainer nicht direkt aufscheinen lassen: Auftreten von nahen Angehörigen, die zunächst Schenkungen in Millionenhöhe von ihm erhalten, das Geld sodann in Form von Kreditverträgen wieder an die Kapitalgesellschaft des Vaters zurücküberweisen

# Fragen?

BK 7.3. - Zentrale Geldwäschemeldestelle (A-FIU)

E-Mail: a-fiu@bmi.gv.at