J5 JOINT CHIEFS OF GLOBAL TAX ENFORCEMENT

GLOBAL FINANCIAL INSTITUTIONS PARTNERSHIP

IDENTITY-BASED CRIME

May 2025

Reference: J5GFIP-IBC

Contents

1. About

I. The Joint Chiefs of Global Tax Enforcement (J5)

The Joint Chiefs of Global Tax Enforcement (known as the J5) are committed to combatting transnational tax crime through increased enforcement collaboration. The J5 is comprised of Australian Taxation Office (ATO), the Canada Revenue Agency (CRA), the Fiscale Inlichtingen- en Opsporingsdienst (FIOD), HM Revenue & Customs (HMRC), and Internal Revenue Service Criminal Investigation (IRS-CI).

The J5 was formed in response to the Organization for Economic Cooperation and Development's (OECD) call to action for countries to do more to tackle the enablers of tax crime. The J5 works collaboratively with the OECD and other countries and organizations where appropriate.

We are convinced that offshore structures and financial instruments, where used to commit tax crime and money laundering, are detrimental to the economic, fiscal, and social interests of our countries. We will work together to investigate those who enable transnational tax crime and money laundering and those who benefit from it. We will also collaborate internationally to reduce the growing threat to tax administrations posed by cryptocurrencies and cybercrime and to make the most of data and technology.

II. The J5 Global Financial Institutions Partnership (GFIP)

The J5 Global Financial Institutions Partnership (GFIP) serves as an international public-private partnership, leveraging the combined capabilities and resources of both public and private sectors to support the J5 mission. By bringing together expertise from across sectors, the GFIP strengthens the joint response to tackling transnational tax crime, delivering an enhanced approach to shared global challenges.

Throughout the year, the GFIP progresses Threat Projects, as commissioned at the Summits. These are developed through multilateral working groups comprised of subject matter experts from both public and private institutions from all J5 countries.

2. Handling advice

I. Protecting this document

The J5 reminds you of your legal obligations in respect of the management of this information, including abiding by relevant data protection legislation in your jurisdiction.

This document has no specific requirements for storage, and it can be considered safe for wide distribution within your organization and for use in staff training or awareness programmes. However, external publication and distribution of this document and its content remains at the discretion of the J5 alone. This document should not be included on public facing websites, external mailing lists, social media or other outlets routinely used by your organization to deliver information to the public without the prior and specific permission of the J5 communications team.

We therefore request that you risk manage any onward dissemination in a considered way.

II. Disclosure requests

Requests for further disclosure which are not permitted by any handling instructions or handling code must be referred to the J5 originator from whom you received this information. Requests for disclosure to third parties under the provisions of the relevant data protection, freedom of information and equivalent legislation should also be referred to the J5 originator from whom you received this information.

III. Reporting suspicious activity

If you identify situations which may be indicative of the activity detailed in this report, and your business falls under the regulated sector, you may wish to report suspicious activity through a SAR (suspicious activity report) or STR (suspicious transaction report). If you decide to make a report in this way, you should adopt the usual mechanism in your jurisdiction for doing so. It will help our analysis if you include the reference J5GFIP-IBC within the text of your report.

The J5 jurisdictions also welcome any information tied to this report which does not constitute a SAR or STR. Please report all such information to your authority via the usual mechanism available in your jurisdiction.

To help us to improve this service, we welcome any feedback you have on both the report itself and the information provided to you. Please email all feedback to j5commsuk@hmrc.gov.uk.

3. About this report

I. Purpose

The Global Financial Institutions Partnership (GFIP) has prepared this report under the guidance of the Joint Chiefs of Global Tax Enforcement (J5). We thank the J5 tax authorities, financial intelligence units (FIU), financial institutions (FI), and banking associations who are subject matter experts on identity (ID)-based crimes for their valuable contributions. The J5 jurisdictions include Australia, Canada, the Netherlands, the United Kingdom, and the United States.

The typology report serves as an informational product, designed to bring awareness to the threat that ID-based crime poses to tax crime and money laundering, in both the public and private sector. It is intended for GFIP members and those within organizations that are involved with the prevention, detection, response and proactive mitigation of ID-based crimes.

This report sets out a general introduction to ID-based crimes, with a focus on synthetic identities. There will be further reports related to more specific areas of ID-based crimes to come.

II. Scope and background

ID-based crime impacts both the public and private sector at the personal and commercial level very significantly. As fraud relating to ID crimes continues to persist, organizations will need to pursue ways to prevent, detect, respond and recover to fraud more quickly and fight it with proactive, multi-faceted, and ever-changing solutions. The J5 is in an opportune position to leverage our partnership, using our structures to share information about current and emerging threats. Such information exchange will enable the GFIP to develop safeguards against those threats, and to make sound decisions across the full range of intervention activity both within and between their organizations.

4. Overview of identity-based crime

I. What is identity information?

ID information, which can include personal and financial data, is a valuable commodity. Cyber criminals employ a broad range of techniques to steal ID information through major data breaches targeted at major data aggregators, as well as large-scale social engineering tactics targeted at the public. As both organizations and individuals continue to be subject to cyber-attacks, it is essential that both have robust safeguards in place to protect themselves from all forms ID crime.

In general, ID information means any information, including biological or physiological information, that is commonly used alone or in combination with other information to identify or purport to identify an individual, including:

- a fingerprint or voiceprint;
- retina and iris images, DNA profile;
- names, addresses, dates of birth;
- written, electronic and digital signatures;
- usernames and passwords;
- credit card number, debit card number, financial institution account number; and
- a passport number, Social Insurance Number, health insurance number, driver's license number.

II. What is identity-based crime?

The terms "ID theft" and "ID fraud" are often used interchangeably, though they differ.

ID theft is the act of stealing ID information with the intent to use the information deceptively, dishonestly, or fraudulently. ID fraud or impersonation is the actual deceptive, dishonest, or fraudulent use of the ID information of another person (living or dead). ID theft is often a necessary precursor to ID fraud.

III. Common behaviours exhibited in identity-based crime

Threat actors involved in ID-based crime may share behavioural characteristics or patterns. Analysis of our data shows that threat actors tend to be:

Patient and organized. They can wait for months - even years - before leveraging compromised information for malicious intent. They obtain personal and corporate information through many different means, including phishing scams, purchasing information on the dark web, and third-party data breaches. Threat actors will combine compromised data with publicly available information about individuals and businesses, like data from federal and provincial corporate registries and details easily found on social media, like birthdays.

Extremely knowledgeable. Threat actors can show a sophisticated understanding of the dependencies between and within organizations. They have a deep understanding of government systems, processes and procedures. This includes online portals, systems and software and operational procedures. They use this expertise to discover new entry points or simply to test methods via trial and error.

Innovative. They evolve their schemes as the public and private sectors strengthen controls. As the complexity of system monitoring increases, they increase the complexity of their schemes. They turn their attention to new programs and continue to target existing government and private sector programs and services. Threat actors continue to test online portals and programs.

This highlights the importance of enhancing security technologies, refining processes, implementing new controls and working within public-private-partnerships to collaborate and bring awareness to new schemes and trends that criminal organizations utilize.

IV. Common methods used in identity-based crime

The methods and most common threats facing the attainment of ID information can be categorised into coerced, complicit or stolen.

Coerced	Complicit	Stolen
People traffickers	Social media recruitment	Insider data theft
Local intimidation	Community participation	Data breaches or leaks
Prostitution	Online crime guides	Hacking and malware
Drug dependence and gambling addiction	Duped by dishonest services (e.g. recruitment or tax refund services)	Ransomeware publication
Blackmail	Promoter groups	Phishing and social engineering Document theft Stolen/hacked credentials sold on the darknet

V. The use of synthetic identities in identity-based crime

Synthetic identities are the use of a combination of real and fake personally identifiable information (PII) to fabricate a person or entity to commit a dishonest act for personal or financial gain. It is the fastest growing form of ID crime and over 80%[1] of all new account fraud can be attributed to synthetic identity fraud.

This type of fraud is different from traditional ID theft, where a threat actor steals an actual person's identity. A synthetic identity may include some pieces of PII from a real person – such as a name, date of birth or Social Insurance or Security number – with fabricated information – such as a mailing address, phone number or email address. As such, there are two main kinds of synthetic identities; manipulated and manufactured.

1 Synthetic Identity Fraud: What is it and How to Combat it (thomsonreuters.com)

The threat of synthetic identities has most notably impacted tax authorities with tax benefit and refund fraud being the target for most criminals involved in this space. This type of tax fraud is often associated with false claims or claims filed on behalf of innocent persons, whose PII has been stolen and bank deposit information or mailing address has been altered, in order to receive the payment. This threat also impacts the financial sector, in particular with new bank account or credit card openings with account takeovers.

It is difficult for a single organization to effectively fight synthetic identity fraud alone. Improved awareness, understanding, data strategy, reporting and information sharing, alongside advancements in technology–such as machine learning and artificial intelligence (AI)– are all helping organizations fight and stay ahead of threat actors.

VI. Common impacts of identity-based crime

It is difficult to quantify the amount of loss connected with ID crimes accurately. Not all cases are reported by victims, whether that be to the government authorities, financial institutions, or other relevant organizations. In a recently published report[2], FinCEN advised approximately 42% of total reports from January to December 2021 contained suspicious activity related to identity, equivalent to $212 billion U.S. dollars (USD). In another report[3], the Canadian Anti-Fraud Centre (CAFC) reported that in 2020, they observed approximately $165 million Canadian dollars (CAD) in reported victim losses, which represents 5-10% of victim losses, as only a small fraction is reported to the CAFC. This increased dramatically to $379 million CAD in 2021, relating to all fraud, ID crimes and associated cybercrime faced by Canadians.

ID crime also has an impact on critical infrastructure and organizational reputation. This is because the primary method to obtain large quantities of identity information is through cyber-attacks, such as large data breaches. This could cause serious harm, including personal injury or death in extreme cases.

There are also other impacts that are hard to quantify for the individual, victim or victimized organization including, but not limited to:

- Vulnerabilities to security infrastructure for organizations
- Resources allocated to safeguard against data breaches
- Psychological concerns - anxiety, depression, suicide
- Emotional resources spent coping with recovery processes - hopelessness
- Erosion of consumer confidence in the marketplace
- Erosion of trust in government and financial sector
- Reduction in quality of life, loss of financial status or income
- Harm to individual reputation (i.e. criminal record)
- Time spent restoring personal reputation
- Harm and time spent restoring financial status

2 Financial Trend Analysis, January 2024 (fincen.gov)
3 PS61-46-2021-eng.pdf (publications.gc.ca)

VII. Mitigation strategies against identity-based crime

Currently, there are existing strategies to mitigate the risk associated with ID crimes. Reducing exposure risks during validation and verification processes prevents criminals from gaining unauthorized access. This includes the use of monitoring and tracking internet protocols to validate legitimate users and multi-factor authentication.

This could also include more validation checks with other issuing authorities (i.e. public to public) prior to opening a financial account and keeping copies of ID cards at account opening with longer retention periods. Another strategy to curb the impacts of ID crimes is device tracking, the use of the same computer, laptop, phone, tablet, or other device to conduct fraudulent activities.

Although controls are commonly implemented to counter external fraud, it is important to protect from internal threats within organizations. This is done through enhanced security personnel screening and systematic checks, as well as implementing appropriate access controls.

Finally, one strategy that focuses on the general population is to conduct educational outreach[4] citizens on how to protect their personal information and not just standard PII, and include social media account information, medical information and other potentially locational or behavioural interests, that criminals may seek to exploit. Internally, organizations have also kept their staff trained on the latest trends, to help recognize and identify suspicious activity.

The following are considerations to improve the ID authentication process and protection measures that can be taken by individuals or organizations, while they handle personal and corporate information:

Stronger authentication processes	ID Theft protection measures
Multi-factor authentication	Secure, shred or black out any paper documents that include PII (bank statements, tax forms and government notices)
Behaviour biometrics	Secure online login information (user IDs and passwords)
Location intelligence	Use digital security software
Device identification	Know the signs of phishing scams
Bot mitigation	Review credit reports
Past fraud risk	Report scams or when accounts or information have been compromised
In-person **K**now **Y**our **C**lient interviews and ID card authentication	Do not share or re-use passwords

4 PROTECTING YOURSELF FROM IDENTITY THEFT ONLINE (ITSAP.00.033) (cyber.gc.ca)

VIII. Financial Risk Indicators

This list identifies *potentially* suspicious or unusual activities and is meant to show types of transactions that *could be cause* for additional scrutiny along with contextual information. The existence of one of these factors by itself does not necessarily mean that the transaction is related to ID crime, tax evasion and/or money laundering.

- Bank account receiving multiple tax refund deposits over multiple days;
- Bank accounts opened shortly before or after the creation or announcement of a tax benefit;
- Bank accounts opened at a location far from client address on file;
- Multiple bank accounts created in a short time frame at same branch or by same branch employee;
- Increased transactions on a previously dormant account;
- Recent password changes to online bank accounts, followed by transfer or withdrawal attempts;
- Repeated use of common names (or very minor variations), mobile phone numbers, email addresses across different customer profiles;
- Same addresses or sequential addresses on same street used to collect multiple tax benefits[5];
- Identical tombstone information (address, phone number, email address) linked to multiple customer profiles;
- Addresses associated with bank accounts that are mailboxes, vacant land or not commonly associated with a household or business;
- Recently updated customer contact information in conjunction with irregular account activity, such as rapid movement of funds immediately after receipt of large refunds or deposits;
- Business bank account receiving tax refund[6] that is not commensurate with size of business, number of employees and normal volume of transactions;

5 IdentityTheft.gov - Warning Signs of Identity Theft
6 Special Bulletin on COVID-19: Trends in Money Laundering and Fraud (canada.ca)
7 ID Theft 11 508 FINAL (fincen.gov)

- Session monitoring:
    - Common IP address is linked to multiple bank accounts in receipt of tax refunds;
    - Common IP addresses or user agent information associated with prior unauthorized account activity[7];
    - Changes in user behaviour as identified with cyber security technology;
- Transaction monitoring:
    - Credit or debit card charges that are considered unusual[8] based on previous history or made in locations abroad that vary from the account holder's home address;
    - High volume of transactions where the difference in the sum of credit and debit amounts is minimal;
- Behavioural monitoring:
    - Sudden increase in debit and credit activity including EMTs, GMTs/wires and deposits, and/or a rapid depletion of funds. Includes a comparison of the customer historical activity to current volumes;
    - High value/high volume – aggregate behaviour including changes in money flow and expected vs actual activity; and/or
    - Internet behaviour including keystrokes, typing speed, screen selections.

8 Credit card fraud - Canada.ca

IX. New technologies and emerging threats

Due to professionalised crime, the modernization of fraud techniques (i.e. use of automation and AI), continued digitization of society and the rise of instant payment,[9] threat actors will continue to target and exploit ID crimes. Government imposter scams constantly evolve, and threat actors continue to develop new tactics and techniques. It is highly likely that the use of ChatGPT and other AI tools to perpetuate fraud will continue to grow as the technology advances and becomes more readily available.

Emerging technologies such as digital ID, enhanced biometrics, AI, and Privacy-Enhancing Technologies (PET) may help mitigate customer ID process exploitations and combat a wide variety of illicit finance typologies. Continued engagement with partners within the public and private sector to explore the utility of available and developing ID solutions, will enable stronger ID processes and counter the underlying drivers of ID-related crime.

9 Instant payments refer to payment applications that are connected to bank accounts that are meant for the quick transfer of funds between registered users, normally with the use of a recipient email or mobile number.

5. Conclusion

This typology report has provided a broad landscape of how ID crimes impact the public and private sector and the GFIP will continue the conversation on this topic. This will be achieved through regular engagement and consultation sessions, in our collective efforts to tackling tax crime and money laundering. It was clear, that through the consultations and virtual engagement discussions for this threat topic, that there are many other opportunities to collaborate on other relevant topics for the GFIP. This report highlighted current trends and financial risk indicators commonly associated with the highest threat of synthetic identities for ID crimes.

As there are other prevalent types of ID crimes - including financial theft and online or cyber theft - the GFIP will continue to produce additional subsequent typologies. GFIP collaboration remains a J5 priority; we know that strategic information sharing and working towards collective solutions across the public and private sectors can deliver mutual benefits and amplify our impact. The continued development and sharing of collaborative typology reports, and/or sharing of domestic products, including the identification of red flags and indicators via the GFIP will help to strengthen anti-money laundering regimes and achieve actionable reporting for both tax authorities, financial regulators and institutions.

6. Appendix A: Case Studies

I. Canada Revenue Agency sample cases

Fraudulent goods and services tax/harmonized sales tax (GST/HST) refunds claimed by development companies

Tax scheme involving an individual who set up two companies portrayed as being in the land development business. This individual then claimed fraudulent GST/HST rebates in the name of these companies on fabricated land development costs. GST/HST cheques received by this individual were deposited to a bank account controlled by another family member from which the funds were withdrawn and subsequently could not be traced.

Fraudulent GST/HST refunds using export provisions

The scheme created and registered 20 corporations and filed for GST/HST refunds. The corporations registered for GST/HST and indicated either at the time of registration, or when contacted, that they were in the business of exporting Canadian manufactured goods to the United States. This resulted in their product being zero-rated (no GST/HST charged on the sales to the United States). Therefore, the exporters were entitled to a refund of GST/HST paid on manufacturing and operating costs. All transactions were fabricated. There was no real business activity. All transactions between the 20 GST/HST registrants were fabricated in such a way as to layer the fraud to avoid detection. There were no physical business addresses. All the addresses provided by the representatives of the corporations were mail drops and all phone numbers provided were cellular.

The names of nominees were used to register for GST/HST, open bank accounts, sign returns, sign company cheques, transact business at financial institutions, etc. For various reasons, most of the nominees were not available as crown witnesses. Amounts were traced to fraudulently claimed refunds to offshore bank accounts in Switzerland and tax haven countries. None of these accounts were in the names of the perpetrators. The remaining funds also appear to have been moved offshore but could not be traced.

II. Canadian Anti-Fraud Centre sample cases

Benefit fraud – victim statement

"Someone hacked my CRA account, applied for the Canada Emergency Response Benefit (CERB) under my name. It was deposited into a false bank account in my name. Then transferred my cell phone number to another carrier, took over my pay pal and accessed my bank account and credit card through there. My credit score continues to fall, and I am unsure as to why."

Data breach – victim statement

"My employer had a cyber security breach back in September 2019. I had been informed by the company that employee data such as name, employee number, Social Insurance Number, DOB, address as well as bank account details were among those that were breached. On May 9, 2020, I had been informed by my bank that someone had gained access to my online account. Suspicious of the access location not being my hometown, the bank had immediately locked-out my online bank account before any unauthorized transaction took place.

"On the following day (May 10, 2020), I had been informed that someone had impersonated me by calling the bank and successfully changed the mailing address. Fortunately, I became aware of this fraudulent activity when I received an email from the bank confirming the mailing address change and was able to stop further activities by the perpetrator."

III. Australian Tax Authority sample cases

Fraudulent tax refund using stolen PII

An individual was sentenced to five years imprisonment with a non-parole period of 18 months for placing false job advertisements online and stealing the identities of job applicants in order to lodge false income tax returns.

Between August 2015 and July 2016, the perpetrator created online job advertisements using names of both legitimate and fictitious companies. Jobseekers would apply for these positions and submit their resumes or CVs. The perpetrator telephoned applicants and conducted phone interviews using various aliases. The perpetrator emailed applicants to offer them a job asking them to provide further details including driver's license, bank account details and tax file number. The perpetrator used the information to assume identities of some victims, lodging 62 income tax returns resulting in refunds being credited to accounts he controlled.

Fraudulent GST refunds using false identities

Multiple syndicate members were convicted of conspiring to defraud the Commonwealth of GST refunds.

The perpetrators were involved in a scheme where confidential taxpayer information was illegally obtained and used to create false entities with Australian Business Numbers and GST registrations. The fraud syndicate then lodged business activity statements (BAS) claiming false GST refunds.

The refunds were directed to bank accounts that had been created using the stolen identities.

The scheme was uncovered by a taxpayer when they conducted a Google search and discovered their personal details located in a spreadsheet.