## Table of Contents



## Related content

Guidance on Managing Family Member/Household Accounts
Photo Identification Guidance
Settlement between the Privacy Commissioner of Canada and Canada Corporation of Manitoba Ltd.

# Guidelines for Identification and Authentication

**June 2016**

*These guidelines are intended to help organizations subject to the Personal Information Protection and Electronic Documents Act (PIPEDA) identify and authenticate individuals in a manner that balances the right to privacy and protection of personal information with the need of organizations to collect, use and disclose personal information for legitimate purposes.*

Trust is an essential component of Canada's economy and the global digital economy. Mutually beneficial interactions between organizations and individuals serve to engender that trust.

Whether in the physical world or online, many organizations develop processes to manage their interactions with individuals. As these processes often involve the collection, use and disclosure of personal information, organizations are responsible for treating that personal information with care and for protecting it in compliance with Canada's privacy laws.

The Personal Information Protection and Electronic Documents Act (PIPEDA) is Canada's private sector privacy law. It requires organizations engaged in commercial activities to collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. It requires organizations to identify the purposes of collecting personal information and limit collection and use to these purposes. Organizations are also required to protect personal information with appropriate security safeguards.

Identification and authentication processes can contribute to mutually beneficial interactions and the protection of privacy rights only if they are carefully designed. An organization that requires personal information about an individual to authorize a legitimate transaction, but needs to ensure that it does not collect, use, retain or disclose personal information that is not necessary for that purpose. Requiring individuals to unnecessarily go through identification and/or authentication processes, or implementing identification and/or authentication in a way that does not take into account privacy rights can result in negative consequences.

This document is intended to help organizations devise methods of identifying and authenticating individuals in ways that respect the rights of individuals to privacy and the requirements of PIPEDA. It is intended to supplement Guidelines for Identification and Authentication the OPC released in 2006.

By respecting individuals' personal information in a manner that shows that organizations will continue to contribute to mutually beneficial interactions, while further strengthening trust in Canada's economy particularly our increasingly digital economy.

## Identification and Authentication: A Primer

The terms identification and authentication are frequently used interchangeably but in fact mean different things. Put very simply, identification involves a claim or statement such as "I am Joe," or the customer associated with this account." Authentication is a verification of that claim.

### Identity, Identity Attributes, and Identifiers

An individual's identity can be defined as the sum of the characteristics that make up who an individual is, such as their name, birthday, where they live or other information. These characteristics are called identity attributes.

An identity attribute can also be an identifier. For example, an individual may be referred to by their name or by a number that is assigned to them. An identifier may be common (i.e., more than one person can have the same birth date) or it may be unique in that it only pertains to one individual.

These concepts, and their distinctions, are important to keep in mind when considering how to develop and implement proper identification and authentication processes.

### Identification

Identification usually occurs when an individual first enrolls or registers with an organization. Establishing identity is the process of linking an identifier to an individual so that he or she can be remembered. Identifying an individual allows an organization to ensure, for example, that an individual's transactions are associated with that account, and that their records are retrievable.

Depending on legal requirements and the context of a business, the identifier that is attached to the individual need not be a "real world" identifier such as a name (e.g., John Doe). It could be an identifier that is only meaningful to the organization, such as a number. Organizations may also create multiple identifiers to identify an individual - but they are distinguishable by how much they reveal about an individual's actual identity.

Some transactions (face-to-face cash retail sales, for example) may be concluded in complete anonymity. Others may require an individual to divulge only some information or identity attributes. In some cases, legal requirements may require that the organization know exactly with whom it is dealing (i.e., banks and other organizations subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, for example).

### Authentication and Authentication Factors

When someone presents themselves to an organization, or their website, and claims to be a customer with whom the business has a relationship, the organization may need to authenticate that claim.

There are different ways to authenticate an individual's identity. These are:

- Something that is **known** to the individual (for example, a password, a personal identification number or PIN, an account number, favourite colour, name of first pet);
- Something the individual **has** (for example, a bankcard, driver's licence, identity card, public-key digital certificate); and,
- Something that the individual **is (or does)** (for example, a biometric, such as a facial image, retina scan, voice print or gait).

In some cases, one of these factors may be used alone to authenticate an individual; in others, combinations may be used. For example:

- Access to e-mail using a password. This represents a **single-factor** authentication process that relies on something the individual **knows**.
- Access to a physically secure area using an identity card with an embedded chip (a smartcard) and a hand-scan biometric. This represents a **two-factor** authentication process. It relies on something the individual **has** (the smartcard) and something the individual **is** (the biometric).
- Access to a physically secure area using a PIN, an identity card with a chip, and a hand-scan biometric. This represents a **three-factor** authentication process. It relies on something the individual **has** (the card), something that the individual knows (the PIN), and something that the individual is (the biometric).

Authentication based on two elements from the same category, for example an account number and a password both fitting that same category, represents more appropriately referred to as multi-factor authentication, not multi-factor authentication.

In addition to the authentication factors listed above, other data such as behaviours or actions that an individual takes (for example, logs on to their account from a certain computer, uses their credit card in a certain location, or conducts well-known patterns) may assist in authenticating an individual.

### Assurances and Authentication

Identification and authentication are fundamentally about the management of risk:

- The risk to the organization of, through bad identification or authentication practices, either denying access to a legitimate customer or giving access to an impostor; or,
- The risk to individuals that their personal information is not appropriately disclosured, and that their identity, finances, or privacy are compromised.

Organizations need assurances that individuals legitimately possess the necessary identity attributes to complete a legitimate transaction. Similarly, individuals need to be assured that only the right people are accessing their account, or conducting transactions using their identifiers, whether in person or online.

Once an individual's identity is properly authenticated, or verified, the organization may authorize a transaction.

## Guidelines for Identification and Authentication

There is no one-size-fit-all approach to identification or authentication. As stated above, these guidelines are intended to help organizations develop appropriate identification and authentication processes.

Although the guidelines are intended to address identification and authentication of individuals by organizations, organizations should also have appropriate processes in place to authenticate employees who have access to customer or client information.

### Only identify when necessary

If there is no legal requirement to do so, or the organization does not intend to maintain an ongoing relationship with an individual, it likely does not need to identify an individual.

Organizations should ask themselves if they need to collect, store, and/or share personal information to authenticate transactions. In other words, is identification necessary to fulfill the transaction? Can the transaction be authorized in a way that is just as secure without collecting any personal information?

**Case in Point**

In PIPEDA Case Summary #2008-394, the personal information collection and recording practices exceeded what was required to verify age and permit entry into the premises. Also see the Summary of the Settlement for this case.

Should organizations determine that identification is necessary for their purposes, it is also important to consider for how long personal information should be retained and how it should be destroyed when it is no longer required for those purposes. See the OPC's Principles and Best Practices for Personal Information Retention and Disposal for further details.

### Determine what identity attributes are necessary to authorize a transaction

If an organization does determine that it needs to identify individuals to authorize transactions, the next question to ask is: what is the minimum amount of information required to fulfill that purpose?

Organizations should ask themselves whether the transaction could be authorized in a way that is secure without collecting unnecessary personal information. For example, rather than collecting and storing a person's full date of birth, a partial date of birth or an attestation that someone is over a certain age may be all that is required.

It is also important to avoid, where ever possible, using numbers such as a driver's licence number or social insurance number as an identifier as they were created for different purposes. See the OPC's Guidelines for the Collection, Use and Disclosure of Social Insurance Numbers and best practices for the use of Social Insurance Numbers in the Private Sector.

### Inform individuals and obtain the appropriate form of consent before identification

Identifying individuals without their knowledge or consent limits their control over their personal information and is contrary to the law. Organizations should therefore seek to inform individuals why their information is being collected.

Consent is strongly tied to the principle that information should only be used for the purposes for which it was collected. If an individual provides personal information for identification or authentication purposes, and it is envisioned that that information will be used for other purposes such as personalizing or customizing the individual's experience, for marketing purposes, for profiling or product updates, or engaging in other forms of relationship building, the individual should be informed of those purposes and their consent obtained either at or the time of collection. In many instances, individuals may be willing to provide the service for which they signed up, without having to agree to these other uses.

Advances in technology have tied to never, less transparent ways of identifying individuals. For example, by analyzing metadata data about individuals organizations may be able to infer information about them providing personal information. (See the OPC's Legal and Technical Overview of Metadata and Privacy).

Metadata could be collected through cookies or web beacons (the OPC's Frequently Asked Questions on Cookies). Device fingerprinting which involves collecting enough information about a device to uniquely distinguish it from other devices, or simply monitoring, which uses mouse, keyboard, Wi-Fi, or Bluetooth signals to uniquely distinguish a device and monitor its location. Since a device is typically associated with the individual who owns or uses it, such technologies can also be used to identify individuals without them being aware.

Without informing individuals or obtaining their consent, such activities may be viewed as being more akin to surveillance and profiling than promoting mutually beneficial interactions that build trust in Canada's economy.

For guidance on different ways of obtaining consent, depending on the circumstances, please refer to the OPC's Guidelines for Online Consent.

### Only authenticate when necessary

An individual should only be authenticated by an organization when it is necessary for the purposes of the transaction. Even if there is a preexisting relationship between an organization and an individual (i.e., the individual has gone through the identification process), then authentication may not need to be invoked in every instance.

If an individual does need to be authenticated, personal information should only be disclosured to that person once the organization is assured that the individual is who they say they are.

**Case in Point**

In PIPEDA Case Summary #2003-155, the transaction did not require authentication and personal information was inappropriately disclosured.

### Ensure the level of authentication is commensurate with risks

The stringency of authentication processes should be commensurate with the risks to the organization as well as to the individual. The higher the risks the higher the assurances an organization will likely need to authorize a transaction. As such, the use of more authentication factors or layers may be appropriate. For example:

- A simple single-factor authentication process may be appropriate to allow an individual to obtain access to some retail or to check the account balance of a loyalty program.
- Obtaining an account balance for a utility bill may require an account or membership number and a numeric access code, (i.e., multi-layer single-factor authentication); or
- Financial services that permit the issuing of payment instructions and making transfers to third-parties may require a multi-factor or multi-layer authentication process.

**Case in Point**

In PIPEDA Case Summary #2003-40, it was found that the collection of additional information was not necessary to establish identity to limit financial risk.

In PIPEDA Case Summary #2009-271, it was found that additional information could have been collected to verify identity and prevent identity theft.

In PIPEDA Case Summary #2006-349, the collection of several authentication factors was reasonable for an organization that handled sensitive personal information.

While the number of authentication factors is important so is their quality. Authentications should not be easily replicated or spoofed. Processes that use commonly known or easily discoverable identity attributes (i.e., birth dates), or one-factor authentication, are more easily taken advantage of by persons who know the individual.

**Case in Point**

In PIPEDA Case Summary #2013-006, a family member who lacked the authority to modify the account was able to do so by impersonating his stepfather.

Organizations should also avoid weak authentication processes, by requiring, for example, passwords that are difficult to guess.

### Ensure employees are properly trained

According to Principles 4.1 and 4.7.4 of PIPEDA organizations are required to train staff about the organization's privacy policies and practices, and to make their employees aware of the importance of maintaining the confidentiality of personal information.

As such, organizations should ensure that all customer service representatives, data processors, and all other employees who have access to personal information receive appropriate training on the importance of privacy and protecting personal information, including the importance of protecting it from unauthorized access and disclosure. Organizations should provide ongoing training on identification authentication policies and processes.

**Case in Point**

In PIPEDA Case Summary #2021-001, a fraudulent transaction could have been prevented with better employee training, as well as proper transactions records.

### Maintain appropriate transaction records

The authentication process should maintain reliable audit records of authentication transactions including the date, time and the outcome. Maintaining such records can assist in assessing risk, as well as demonstrating compliance with applicable privacy laws. The level of detail in the audit logs, as well as the retention period for data, should reflect the risks associated with the information or service. Audit records should not contain personal information, but rather record authentications, but should not contain the actual authentication information (i.e., passwords or PIN).

As well, audit records need to be protected since they can create data trails that can reveal information about the individuals' transactions, when linked with other identifying information, could constitute personal information under PIPEDA. Audit logs should therefore be treated with the same protections as other personal information.

### Continually assess threats and mitigate risks

Organizations should regularly reassess risks and threats for each service delivery touch point and deploy appropriate risk mitigation measures, including adjusting the strength of authentication processes, to address changing threats. This entails keeping abreast of changes in business practices and technologies that either strengthen existing authentication processes or undermine them.

For example, organizations should have systems and procedures in place to address man-in-the-middle attacks where a fraudulent actor intercepts communications between an organization and an individual. Organizations should also have plans in place to address phishing, where a malicious actor attempts to trick an individual into disclosing their identifiers or authentication factors.

In addition to the due diligence required of organizations to mitigate risk, it is also important that organizations be aware of the consumer protection laws that protect Canadians from fraud, misleading ones, anti-spam, and forward prospecting and prevent phishing their PIPEDA or passwords. All the same time, organizations should not overlook more conventional low-tech threats.

**Case in Point**

In PIPEDA Case Summary #2012-004, an imposter used social engineering techniques to gain access to an account.

PIPEDA Case Summary #2007-377 demonstrates the importance of adapting policies and practices to mitigate new risks and ensuring employees are properly trained and follow customer authentication procedures in order to adequately protect personal information.

### Protect personal information

Organizations should have policies and practices in place to manage risks to the personal information they hold. Security safeguards must be commensurate with the sensitivity of the personal information and the risks associated with it. For more information see our Securing Personal Information Self-Assessment Tool.

Given the potentially sensitive nature of identity information, organizations should also have a plan to notify individuals should there be a security breach so that those individuals can take the necessary steps to protect themselves from identity theft. For more information see Response to a privacy breach at your business.

It is important to note that S-4 (The Digital Privacy Act) received royal assent in June 2015 and the amendments dealing with breach notification and recordkeeping will come into force shortly. Please check once the related regulations outlining specific requirements are developed and in place.

### Rely on trusted identity documents or credentials

As a means of authentication, identity documents or credentials (for example, identity cards, drivers' licences, passports, etc.) can be used with more confidence when their genuineness can be verified. In general, the issuer of the document is in the best position to assess the appropriate reliance to place on a credential.

Ideally, they should only be used for their original intended purpose. In other situations, an organization should only rely on them when it has some assurance of the integrity of the issuance process. For example, relying on a driver's licence from a foreign country may carry more risks than relying on a licence issued in Canada. Organizations may also rely on e-credentials or tokens from trusted sources, preferably if they have already entered into agreements with them.

### Rely on trusted parties when outsourcing identity management

Under PIPEDA, an organization is responsible for personal information under its control, including information that has been transferred to a third party for processing.

Therefore, in situations where an organization outsources identification or authentication functions to a third party, the organization should ensure that the third party provides a level of protection the organization considers to be at least comparable to its own. Should this organization remain responsible, through contractual or other means, for ensuring that identification and authentication processes meet its requirements and reliably protect personal information.

Organizations that outsource identity management to third parties should inform their customers of this practice. Third party organizations that act as identity management providers should also collect, use or disclose personal information in accordance with these guidelines.

### Permit individuals to control their identification and authentication information

Organizations should offer individuals options to manage their identification and authentication information. When possible, individuals should be allowed to choose their:

- Own identifier and should not be required to only use their name. However, there may be situations, such as when a person is dealing with a medical institution, where using a pseudonym specific information and the use of a nickname or other alias/identifier is not possible;
- Passwords or PINs, including those that exceed a standard minimum length and complexity; and,
- Questions and answers when personal information is required for authentication.

Where reasonable and appropriate in the circumstances, organizations should also provide enhanced authentication processes to individuals who request them.

### Consider the use of biometrics carefully

Before considering the use of biometrics (such as automated facial recognition technology, retina scans, fingerprints, hand-print or their gait) management systems, organizations should consider whether they are necessary, effective, and proportional to the potential privacy risks, and whether there is a less privacy invasive way to identify or authenticate an individual. See Acting with Integrity: Biometrics and the Challenges to Privacy for an overview of privacy issues related to biometrics.

Although they can be strong identifiers (i.e., a fingerprint is a unique and persistent identifier that corresponds to one individual) the vast majority of timeof they are far from being a panacea. For example, they are not secrets, they can be observed and copied, they can change over time (e.g., due to age or injury), depending on how unique and persistent a biometric is, and how effective the technology used to gat matching, automated recognitions systems may produce false positives or false-negatives.

Unlike a password, if a biometric is stolen or compromised it is very difficult, if not impossible, to change. If there is a risk that a biometric could be compromised, it should not be used for authentication on its own. It should be used with another authentication factor, such as something only the individual has or knows.

When appropriate, biometric information should be locally stored (i.e., on a device) rather than in a central database. Centralized biometrics increase the risk of data loss or the inappropriate cross-linking of data across systems. Local storage, such as mobile phones or smart cards, by contrast, gives individuals more control over their personal information.

By its very nature biometric information is sensitive information and should be protected by appropriate safeguards, including for example, encryption.

**Case in Point**

In PIPEDA Report of Findings # 2013-012, the immediate transformation of a biometric into an encrypted binary template rendered the biometric difficult to interpret by other parties or applied to other purposes. The raw data the biometric image was not retained.

In PIPEDA Case Summary #2008-391, a biometric was converted into "a matrix of numbers that represent the behavioural and physical characteristics of the way the individual speaks." The representations were stored in a secure database and access was highly restricted.

Organizations should always seek explicit consent to collect biometric information and give individuals the choice not to use their biometric information for identification or authentication purposes when there are reasonable alternatives.