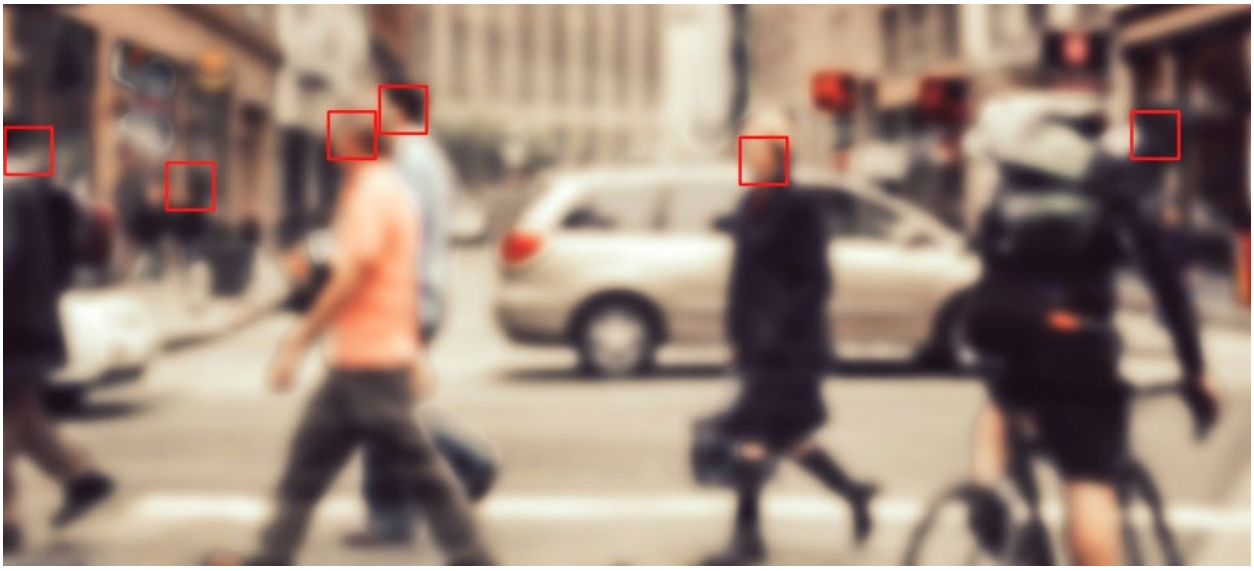
What is PII? Personally Identifiable Information

By: Eugene Bekker



You may see the acronym PII used when talking about security, privacy, and data breaches. It stands for personally identifiable information, which is personal data that can be used to uniquely identify a specific individual. PII is usually sensitive and private information, such as your Social Security number, bank account number, driver's license number, physical address, even your full name and your date of birth. The list is not exhaustive. It also includes medical, educational, financial, employment and any other information that can be used to identify you by itself or when combined with other information.

If you've been keeping eye on the news surrounding identity theft, data breaches, ransomware attacks, personal or online privacy, you have probably noticed personally identifiable information is often referenced. While this term might seem straightforward, it's more complicated than you think. And, having your PII compromised by scammers can be harmful to your personal and financial profile.

The National Institute of Standards and Technology (NIST) defines PII as information that can be used to distinguish or trace the identity of an individual, whether directly or combined with other personal or identifying information that is linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

PII is significant because, whether lost, stolen or exposed, it is how identity thieves can perpetrate their crimes. Sometimes all it takes is one or two pieces of information to compromise a person's identity. Still, not all PII is considered equal.

WHAT INFORMATION IS CONSIDERED PII?

Some pieces of information are unique to you, and you alone. PII in this context is often referred to as "sensitive." These are the identifiers that identity thieves are most interested in capturing, and it may include your:

- **Personal identification numbers:** Social Security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number or credit card number
- **Personal address information:** street address or email address
- **Personal telephone numbers:** home phones or mobile phones
- **Protected health information (PHI)**: medical record numbers, medical histories, test results, health insurance beneficiary numbers or payment information for healthcare services
- **Payment Card Industry (PCI) Data:** credit card numbers, or other bank card or financial information
- **Personal characteristics:** photographic images (particularly of face or other identifying characteristics) or handwriting
- **Biometric data:** fingerprints, retina scans, voice signatures or facial geometry
- **Information identifying personally owned property:** Vehicle Identification Number (VIN), home or vehicle title number
- **Asset information:** Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person

Other pieces of data by themselves aren't considered PII because they could be shared with other individuals. This information has become known as "linkable." By combining them together, or linking to one of the above examples, they can be equally as appealing to fraudsters…and equally as harmful if exposed. This type of PII may include your:

- **Date of birth**
- **Place of birth**
- **Business telephone number**
- **Business mailing or email address**
- **Race**
- **Religion**

- **Geographical indicators**
- **Employment information**
- **Medical information**
- **Education information**
- **Financial information**

WHAT DO CRIMINALS DO WITH PII?

There are several malicious ways that cybercriminals and identity thieves may use PII. Through direct attacks, they can apply for loans or lines of credit, make purchases with your credit cards, steal your tax refunds, drain financial accounts, or more.

Another way that PII may be used is to commit synthetic identity theft. Synthetic identities are created when a fraudster combines someone's Personally Identifiable Information with fake details, and/or personal information from other individuals. For example, one individual's Social Security number might be cobbled together with a fake name and address as well as another real person's driver's license to create a new identity. According to the FBI, synthetic identity theft is the fastest-growing financial crime in the U.S.

The third way that criminals may use PII is by selling the stolen data on the Dark Web. Everything from social media credentials and credit card numbers, to medical records and Netflix passwords, can be sold by bad actors for criminal and financial gain. Hackers can make a pretty penny by capturing and offloading data.