Identity Theft Coverage

Identity theft occurs when someone uses elements of your personally identifying information (PII), such as a Social Security number or financial information, to commit fraud. Many consumers assume identity theft means using a stolen credit card, but this should be the least of your concerns. Identity theft is widespread and involves many other factors that can put you at risk.

What is Identity Theft?

Identity theft occurs when somebody uses your personally identifiable information (PII) for his or her own financial gain. In most cases, thieves gain access to your bank account, credit or debit card. However, your mobile, telephone, online, and insurance accounts are also susceptible. Even your tax returns are open for attack. Data breaches, such as those of major retailers and online sites, are a major source of personal information, which is why two-thirds of identity fraud victims were notified about a data breach in 2014. However, since it can take years for identity thieves to piece information together, a data breach in 2012 might not result in identity theft until years later.

Why Choose ID Watchdog Identity Theft Protection?

- The average victim spends 330 hours and $9,650 resolving his or her own case. Many victims lose far more.
- Florida ranks #1 for highest number of identity theft complaints with Miami-Dade listed in the top 3 counties.
- 50% of Identity theft victims have trouble getting loans or credit cards.
- 12% of victims have had arrest warrants issued in their names.
- Identity theft occurs every two seconds in the U.S.
- Without identity theft protection, children won't know if their identity has fraudulent activity until they reach the age of 18 and apply for credit.
- Social media users are twice as likely to become a victim of identity theft.
- Smartphone users have a 33% higher risk for identity theft.

What Information is Valuable to Thieves?

Your personally identifiable information is what thieves value the most.

- Your name, address, Social Security number, and date of birth are the Holy Grail of identity theft. With these pieces of information, thieves can open new accounts, file tax returns, or get medical care in your name.
- Credit card and debit card information is valuable in the short term because it's easy to make purchases before anybody notices.
- Bank account information can be used to withdraw money or make purchases.
- Email accounts can be accessed so that thieves can lock you out of your account or redirect emails to gain access to sites with your financial information.

>> Benefit Eligibility Note:

- **All M-DCPS Full-Time and Part-Time employees, and Retirees are eligible to enroll in the identity theft coverage offered by the School Board.**
- **COBRA participants are ineligible for identity theft coverage enrollment.**
- **See eligibility information for more details.**

Identity Theft Coverage

- Online accounts, such as Amazon, subscription websites, and any site where you store payment information, can be used to access not only the account but also others with similar passwords or linked email accounts.
- Mobile phones can be used to access information, make payments, make calls, and even commit crimes.

Who is an eligible dependent under this coverage?

Eligible dependents covered under the this plan include:

- Spouse (until a final decree of divorced has been filed)
- Domestic Partner
- Unmarried natural children, stepchildren, children under your care through court-approved guardianship, and children of a domestic partner through the end of the calendar year in which he/she reaches age 20.
- Children may be covered until the end of the calendar year in which the child reaches age 26 if he/she is a full-time or part-time student who receives more than half of his/her financial support from the eligible employee. Children may also be covered until the end of the calendar year in which he/she reaches age 26, if the child suffers from a mental or physical handicap, is incapable of self-support, and is fully dependent upon the employee for support.

How Thieves Obtain Your Information?

The majority of personally identifi able information is released in corporate data breaches, such as those aff ecting major retailers (e.g., Michaels, Target, and Nieman-Marcus) and online subscription sites (e.g., Ashley Madison). However, there are other ways for thieves to harvest your information:

- Using malware, such as keylogging programs and other spyware, allows thieves to obtain information stored on a computer, phone, or tablet.
- Off ering fake or hacked free WiFi connections allows thieves to redirect your browser from your bank, ecommerce, or subscription site to a data collection site that looks just like your usual landing page but records your account name, password, and PIN.
- Buying used smartphones that haven't been properly wiped and reset. Recently, a security company bought used smartphones and ran a data recovery app to uncover a wide variety of personal information despite the phones being reported as cleared of all data. Email accounts, personal photos, and logins to websites, including banking sites, were all available.
- Physically stealing credit cards, bank information, identifi cation cards, passports, driver's licenses, and loyalty cards through pickpocketing, burglary, or mail theft.
- Using RFID readers allows thieves to acquire credit card and passport information without contact.
- Watching people log in or enter credit card information in a public place (often called shoulder surfi ng).
- Impersonating trusted organizations in emails, SMS, phone calls, or any form of communication is done by thieves in order to get someone to disclose personally identifi able information (often called phishing).

Unfortunately, there are many more ways for thieves to obtain your personal information. The only way to remain truly protected is to enroll in an identity theft protection service, such as ID Watchdog, to monitor your personal information and alert you of any suspicious activity.