WINSTEAD

Retirement Plans at Risk for Identity Theft

09.27.17

While many cyber threats have special names, e.g., ransomware, malware, cryptolocker, advanced persistent threats or GRIZZLY STEPPE (a malicious cyber attack that occurred late in 2016), your retirement plan's data may be most at risk from common things an employees do every day that put themselves at risk for identity theft. It is those common things, discarding paperwork with personal information, postings on various websites and other information that can be available in the public domain that identity thieves may use to gain access to an individual employee's retirement plan account. Retirement plan accounts have been stolen by identity theft in several incidents. A retirement plan is at risk because the correct participant may still make a claim for his benefit and the plan's terms would provide for such benefit, even if the retirement plan or its record keeper fell for the false claims of an identity thief and paid the benefit to the wrong party.

In order to protect the personal data and the retirement plan accounts of your employees, in addition to IT security and strong contractual protections with vendors, employers may want to remind employees to guard their personal documents, passwords and keep personal information confidential. This may include a variety of steps, such as:

- Shredding documents before disposal;
- Regularly checking their retirement plan account to verify that no unauthorized transaction has occurred; and
- Reading all correspondence related to their retirement plan account.

In one situation, a soon to be ex-spouse was caught obtaining the other spouse's retirement account assets and will get to experience life in a jumpsuit for five years, barring early release for good behavior. Not all identity thieves are caught and some have been successful in obtaining retirement plan accounts to which they were not entitled.

Employers and plan sponsors should carefully review their vendor agreements and your plan's record keeper's procedures on identity verification to determine if there is adequate protection for the employees' retirement plan accounts against identity thieves and for the plan sponsor to protect the plan's assets. If a retirement plan vendor erroneously pays an account to an identity thief, the participant would still have the right to make a claim for his or her retirement account from the plan. So while retirement plan (and health plan) data protections are very important, it is also important to ensure that the retirement plan benefits are also protected against the work of identity thieves and this requires protective procedures in the human resources or benefits department and all the way through and including the retirement plan vendors.

Employers and plan sponsors should review their internal security procedures such as verifying the identity of employees who call in with questions, security policies, breach or suspected incident emergency response protocol and procedures, and cybersecurity insurance, including reviewing the policy's exclusions. While insurance may be available, the value of such insurance may vary greatly and exclusions may limit its usefulness. States have continued to add breach notification laws, and some Circuit courts have made it easier for a person whose identity is stolen to bring suit, increasing the risks and costs associated with litigation alleging failure to protect identifying information.

Contacts:
Greta Cowart
214.745.5275
gcowart@winstead.com
Marsha Clarke *(Admitted in MO and IL)*
214.745.5877
mclarke@winstead.com
Nancy Furney
214.745.5228
nfurney@winstead.com

Lori Oliphant
214.745.5643
loliphant@winstead.com