



THE AUDITOR'S REPORT

NEWSLETTER

A Publication of Nearman & Associates, CPAs, P.A.

Protecting Member And Employee Information From Identity Theft

According to the FBI, identity theft is one of the fastest-growing crimes in the U.S. Studies show that about 1 in 5 families in the U.S. has been a victim of identity theft. It can occur in a variety of ways, including, stealing Social Security or credit card numbers and then changing the address on bills, using information to impersonate the victim and then rent or buy products, using personal information in criminal acts.

Worst of all, the victim doesn't even know they have become a victim of this federal crime until months later, when they are turned down unexpectedly for a loan, or get a call from a collection agency about an account they never opened, or worse yet, a call from the police about a crime they didn't commit. Don't let your credit union be an unknowing participant in this crime. Ensure that members' and employees' information is protected.

What can a credit union do to adequately protect its members, employees, and itself from being a victim of identity theft? The number one priority is to define sensitive member and employee information and where it is used or stored. Below are some internal control suggestions to consider when reviewing the credit union's overall efforts to safeguard member information and to deter identity theft:

Member Information: To protect the credit union's members, the following steps should be considered to properly safeguard member information:

- ▶ New Accounts - verification procedures for new accounts should include, as appropriate, steps to ensure the accuracy of the application information.
- ▶ Address Changes - adequate verification of address changes is necessary to reduce the likelihood of identity theft.
- ▶ Loan Applicants - a careful review of loan documents can detect irregularities that create "red flags" to identity theft. Is the social security number on the application different than the credit report? Do the addresses differ on the loan documents? Do employer names differ?
- ▶ Conduct "systems penetration tests" to determine if systems are hacker proof. Filters, firewalls, encryption, authentication, and monitoring software are essential tools for information security.
- ▶ Provide training to all employees on security and privacy protection.
- ▶ Conduct criminal and civil background checks before hiring all employees who will have access to personal information.
- ▶ Prohibit using birth dates, social security numbers, or drivers' license numbers as account or personal identifier numbers.
- ▶ Restrict system access to sensitive personal data to only those who need to know the information.
- ▶ Adopt secure methods of disposing of sensitive information. A strict policy should be in place that describes the methods to properly dispose of sensitive and confidential data. If third party providers are used, ensure an adequate contract is in place, the vendor screens its employees, has adequate liability insurance, and follows prudent and acceptable procedures to dispose of your records. In addition, determine that the vendor's physical security methods are sufficient, and that they maintain accurate and current records to provide the necessary audit trails of destroyed records.
- ▶ Physical security - it is imperative to lock up sensitive and confidential information and restrict access to only those with a need to know.

Employee Information: One of the single most underlying sources of identity fraud is the theft of employer records. To protect the credit union's employees, the following internal controls should be considered:

- ▶ Lock up and limit access to personnel files, and minimize the types and amounts of data stored on employees.
- ▶ Provide a secure place for employees to maintain their purses, papers, briefcases, etc., at work.
- ▶ Don't use social security numbers as employee identifiers, or on paychecks, namecards, staff badges, etc.
- ▶ Consider using temporary employees only in areas where confidential information cannot be accessed.
- ▶ Tighten scrutiny of third-party vendors having access to personnel information. Since vendors increase the number of people who will have access to personnel information, verify that vendors are just as committed to protecting confidential employee data as you are.

Credit unions have legal and business incentives to set up effective policies, procedures, methods, and practices to keep information thieves from robbing their members and employees' identity. Credit unions also have incentives to protect themselves from liability. Don't let your credit union be the source of stolen information used against those it seeks to serve. ♦

Christopher J. Vallez, CPA, MBA, CICA
Partner