



Insurance agents and BGAs are entrusted with a great deal of financial and other personal information by policyholders. That information is valuable, not only for your business purposes, but also to identity thieves. As the custodian of this data, you are responsible for safeguarding it. BY JEAN FEINGOLD

THEFT

PRECAUTIONS

Protecting your clients, your employees,
and your business

Anyone who is in contact with your physical premises or your computer files has the potential to steal your data.

What thieves want and how they use it

Identity thieves like all kinds of information about people. While Social Security and credit card numbers are popular, what they really love is reportable information, noted Bill Dixon, director, Enterprise Security Services, for Mutual of Omaha subsidiary Continuum Worldwide. This includes names, addresses, phone numbers, and birth dates. "Any combination of these is like gold for an identity thief," he said. These basic facts let thieves discover almost any personal information stored in a database.

Beyond the obvious misuse of stolen credit cards to make purchases, stolen identities can be used by illegal workers to get jobs, by uninsured people to obtain healthcare, and by criminals during arrests. This false data then becomes part of the victims' records. Potential negative consequences for identity theft victims include ruined credit, arrests for crimes they did not commit, loss of Social Security benefits, and inaccurate medical records. It takes the average victim 600 hours of their own time to get their records corrected.

How information is stolen

"Anyone who is in contact with your physical premises or your computer files has the potential to steal your data," stressed Certified Identity Theft Risk Management Specialist (CITRMS) John R. Hall, president of IDT Professionals. In addition to employees, this includes ven-

dors and subcontractors like IT consultants, payroll companies, cleaning services, shredding companies, copier and computer repair techs, CPAs, security alarm services, and security guards.

Staff carelessness can make data vulnerable to theft. Taking home laptop computers and files removes them from in-office security protections. Thieves also attack using pretexting or social engineering. "This means that they are either pretending to be someone who should be given access to the information or using habits of your clients to get their information," Hall said. Insurance agencies must improve the checks they do to make sure the person really is their client, not someone pretending to be him or her. This is particularly important during phone and e-mail contacts.

Thieves are most likely to target a company's weakest link, which is usually people, Dixon agreed. "For example, phishing targets the vulnerability of a person," he said. "For the technical breach to happen, most often there is some interaction with a person to kick it off. Inadvertently, employees or consumers will let identity thieves into our information and we don't always know it."

Legal responsibilities

Two federal laws regulate companies offering credit regarding protection of customer information. While the Red Flags Rule in the Fair and Accurate Credit Transaction Account Act of 2003, which covers accounts in

which periodic payments are made, does not explicitly mention insurance agencies, they would be well advised to follow its guidelines. The legislation states that companies must look for red flags like credit report fraud alerts, address discrepancies, and identity theft victim notices when extending credit to make sure the account applicant is genuine. Should a breach occur in an insurance agency, it will be up to that agency to prove it took the necessary steps to protect their data.*

The Gramm-Leach-Bliley Act of 1999 requires financial institutions, including insurance companies, to protect the security and privacy of clients' personal financial information by sending privacy notices, developing a plan to protect policyholders' information, and providing on-going training. How companies should comply with these laws is not always clearly specified. Insurance brokerages must develop and use thorough data protection plans while documenting everything they do to this end.*

Understanding the data is crucial. "If you don't understand the data, there's no way to know what is the appropriate protection to put around it," Dixon said. "The organizations that are gathering this information, they see it every day. It's the information they need to conduct business. But it's also highly sensitive information that can cause potential harm if it falls into the wrong hands, not only to the customers but also to the organization."

Hall recommends an organized system to prevent identity theft. First the brokerage should select an information security officer. This could be the chief information officer, the chief privacy officer, or the person managing compliance issues. "Look inside your organization

and find someone who has a vested interest in the prevention program succeeding and has access to the top level of the company," he stressed. Unless top management understands both the personal and corporate liability of doing this incorrectly, there will be insufficient buy-in to the prevention program by other staff.

Next written policies and procedures creating an identity theft prevention program must be devised and implemented, Hall said. This program must ensure that all computer networks and paper file storage containing corporate, client, and employee information have appropriate security and access control procedures. The vendor management process must ensure that appropriate data protection language is included in all vendor contracts. Conduct due diligence to ensure that vendors have proper controls in place and are following the requirements. The program should also include oversight into privacy and information sharing policies and practices. Requirements for reporting issues and consequences for failing to follow these policies must be specified.

Training is key

Perhaps most importantly, a training program for all employees must be conducted, preferably by a CIT-RMS, Hall said. It should cover proper handling of sensitive information to prevent theft, identify Red Flags, and protect privacy while emphasizing the risks and liabilities of data loss. This training should be given once to existing employees and new hires and then repeated annually, with regular reminders of how to handle sensitive information provided through employee newsletters and e-mail blasts. Permit physical and computer data access only to

Even with the best precautions, breaches occur and confidential information is lost.

trained employees and discontinue access when they leave.

When training is completed, Hall said each employee must sign a "Use of Confidential Information by Employee" form to demonstrate they have been trained in handling private information. These forms, vendors' signed contracts, the written policy, and every other document showing what is being done to safeguard data must be kept on file to demonstrate the brokerage is taking reasonable precautions and working actively to comply with federal law.

If a breach occurs

Even with the best precautions, breaches occur and confidential information is lost. Currently, 44 states have breach notification laws, but notification should be done everywhere. "If there is a breach of information of a resident of one of those 44 states, notification must be sent to them," Dixon said. Typically these notifications explain what information was lost and how, offer an apology, and recommend that affected consumers monitor their credit reports to make sure their information



In the insurance industry, they're selling trust, so a trust has been breached along with the information. The brokerage's image can be tarnished and that's hard to recover.

is not being fraudulently used. Many companies provide free credit monitoring for a year.

Law enforcement should also be notified of any breach, Hall said. Despite this, if identities were stolen and used, the burden

of correcting the problem falls on the victim. Kroll provides the only identity restoration and monitoring service he recommends and brokerages may wish to offer it to their clients proactively.

Even if lost data is not used by thieves, significant damage is done to the company. The cost to a company whose information is breached averages \$197 per account breached, Dixon noted. This includes mailing breach notification letters, employee time to repair data and add new security, and lost revenue opportunities, but does not include legal costs. "The consumer's reaction could be, 'I don't trust them anymore,'" he pointed out. "In the insurance industry, they're selling trust, so a trust has been breached along with the information. The brokerage's image can be tarnished and that's hard to recover." Both current and potential clients could be lost.


There is also a fairly high risk that clients whose identities were stolen will sue the brokerage. "If they're the point of breach, there's a strong chance they may have to face litigation by the carrier whose policyholder was breached and the policyholder himself," Dixon pointed out. "They're a key component if they were the ones with the lax policy or the lax security when the breach occurred."

Prevention is best

"Putting practices in place to detect, prevent, and mitigate identi-

ty theft of your clients shows that you are taking reasonable steps to prevent this from happening," Hall said. "It also shows you are taking reasonable steps to prevent inappropriate use of said information. In the event that someone does become the victim of identity theft or some data is lost, stolen, or inappropriately used, this is an affirmative defense against potential lawsuits."

"The unfortunate thing is it's really hard to make things right once a breach occurs," Dixon commented. "If brokerages want to retain that business, they need to provide that level of assurance they're doing things correctly. If they were lax, maybe because they thought it cost too much, they must remember—this is the critical part of your business. This is definitely an investment where you must be proactive. Any type of breach, especially one of a magnitude where someone's personal information is being used, means any trust factor has gone out the window. As a policyholder, I want to know they're doing the right thing with my information."

"Identity theft is a huge business and that's what it is, a business," Dixon continued. "There's a lot of dollars involved. On the good side, this is where organizations can show they're doing something through due diligence and the programs they institute to prove they are serious about protecting the privacy of their policyholders." 

*If you have any questions about your agency's risk, please contact your counsel.

Jean Feingold is a Gainesville, FL-based freelance writer. Her work has appeared in many trade magazines. She holds an MBA in management from the University of Florida and a BA in psychology from New College.

