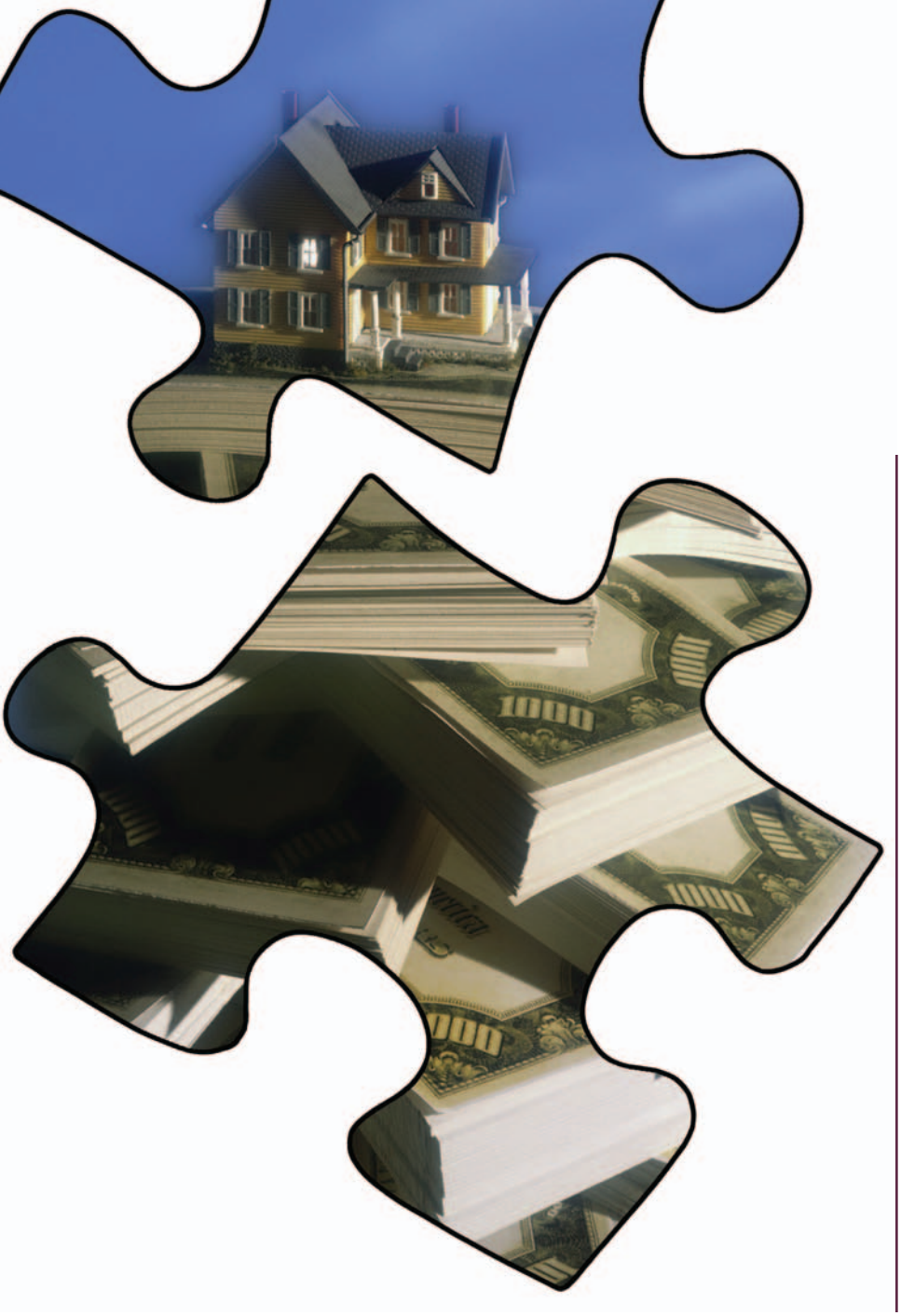


fraud alert

april/may 2005

Mortgage fraud is bringing down the house

Eyes on the spies

Feds attack shady spyware vendors

Crime doesn't have to pay

You can help prosecutors nab bankruptcy fraud perpetrators

Background checks can protect your business

FTC rules define, clarify identity theft procedures

McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

105 W. Madison Street, Suite 406
Chicago, Illinois 60602

Mortgage fraud is bringing down the house

It may seem fairly innocuous when prospective property buyers fudge their incomes a little or fib on the source of their down payments. But according to the FBI, mortgage fraud, if left unchecked, is poised to become the next savings and loan crisis.

In 2004, the bureau called on the U.S. House Financial Services Subcommittee on Housing and Community Opportunity to join in supporting mandatory reporting of fraudulent activity in the mortgage industry, as well as safe harbor provisions to protect informants.

Fraud runs rampant

Between 2001 and 2004, FBI mortgage fraud investigations increased more than fivefold. And mortgage industry sources reported more than 12,000 cases of suspicious activity during the first nine months of 2004 — triple the number reported in all of 2001.

Based on its own investigations and the reports it receives, the FBI estimates that 80% of mortgage fraud is fraud for profit. It involves industry insiders such as appraisers, accountants, attorneys, real estate brokers, loan originators, mortgage brokers and underwriters. The other 20% is fraud for housing, in which borrowers act alone in falsifying application information to qualify for loans.

Both types of fraud are costly, not only to financial institutions left holding worthless collateral but also to innocent consumers lured into buying property at artificially inflated prices. The price tag runs well into the millions every year, the FBI says, warning that skittish investors may eventually require higher returns from their mortgage-backed securities. That could ultimately lead to higher interest rates and a smaller mortgage-loan funding pool.

Three schemes prevail

Because the potential for loss is greatest with organized fraud, the FBI is focusing its preventive efforts more intently on mortgage fraud for profit. There are three major scams at work in the mortgage industry today:

Equity skimming. This fraudulent practice takes several forms. In one scheme, perpetrators deed property on which a lender is foreclosing to shell companies. The shell company then declares bankruptcy. Title transfers can be repeated several times and bankruptcies can be filed to cover all of them.

Another equity-skimming scam uses threats of foreclosure to dupe homeowners into paying amounts equivalent to the equity in their homes to fraudulent lenders.

Property flipping. This swindle uses artificially inflated appraisals to quickly resell a recently acquired property for a considerable profit. It may involve identity theft, straw (or fake) borrowers and industry insiders.

Identity theft. With advances in computer technology and the ready availability and anonymity of online sources, corporate and professional identity theft is on the rise. Perpetrators adopt a business's employer identification number to secure commercial loans or corporate leases.

Location counts

Mortgage fraud is a nationwide problem, but the FBI says it is worse in some areas of the country. As of September 2004, Georgia led the list of states the FBI cites as those with the highest number of mortgage fraud reports. (Florida, Nevada, Utah, South Carolina, Michigan, Illinois, Missouri, California and Colorado round out the top 10.)

Hot real estate markets in a cool economy are open invitations to fraudsters. The prime targets are neighborhoods that are being gentrified — because they represent excellent opportunities for flipping — and those that attract immigrants who are unfamiliar with U.S. real estate practices.

What authorities are doing

Lenders are working more routinely with the FBI, the federal Department of Housing and Urban Development, Fannie Mae and other agencies and organizations to prevent, identify and deter mortgage fraud.

The FBI is collaborating with industry organizations to increase awareness of the problem and to improve access to investigative personnel when fraud is suspected. Additionally, the FBI has developed a national computer system to identify companies and individuals with histories of property flipping, and is using undercover operations and court-approved wiretaps to flush out perpetrators.

In 2004, the bureau consolidated its mortgage fraud activities into the Financial Crimes Section of the Criminal Investigative Division and adopted its overall strategy of focusing on insiders while partnering with state and local law enforcement to combat mortgage fraud.

One step remains

Agency officials believe one key step remains: legislation or regulatory commission orders for a mandatory fraud reporting mechanism. With mortgage fraud scams potentially topping a billion dollars a year, they say it's a weapon they sorely need from Congress or a federal regulatory agency.

Eyes on the spies

Feds attack shady spyware vendors

Computer pop-up ads were bad enough even before their originators started tailoring their marketing with spyware, or secret programs that tracked recipients' online surfing habits. Things got worse when perpetrators began using keylogger programs — which record user keystrokes — to obtain personal information for fraudulent purposes, such as identity and credit card theft.

Now, the Federal Trade Commission (FTC) is pursuing its first complaint against spyware vendors.

Risky business

Spyware, or programs Web surfers unknowingly install on their computers by clicking on links, downloading free offers such as screen savers, or opening other applications, can range from the annoying to the truly damaging. More innocuous programs can be removed with free software available on the Internet. But many nefarious programs are equipped with reinstallers that reload threats as soon as they are removed.

For the FTC, the last straw came when businesses started creating spyware simply so they could sell consumers the means to remove it. The regulatory commission filed suit last October against three

Who's watching whom?

Say "spyware" and the first things that come to mind are fraud, identity theft and annoying pop-up ads. While all of those uses are growing, the most common use for spyware may surprise you.

According to SpywareGuide, an online spyware tracking and privacy service, the biggest users of keylogger programs — which record keystrokes to track someone else's computer trails — are spouses spying on their mates. In some cases, both spouses have keyloggers tracking the other person.

Parents monitoring their children's Internet activity is another popular use for keyloggers, though SpywareGuide notes that a keylogger telling parents where their kids have surfed is no substitute for parental supervision.

Adopting a "turnabout is fair play" attitude, a growing number of computer-savvy children are using keyloggers to monitor their parents' machines — most often so they can get passwords to unlock parental controls.

Some bosses use keyloggers to monitor employees' activities, though such scrutiny should be made known to employees to reduce the risk of litigation for invasion of privacy. Businesses may not legally use spyware to steal competitors' trade secrets, but that doesn't mean it isn't happening. Rampant corporate espionage makes it imperative that companies keep antispyware technology up-to-date and in constant use.

companies: Seismic Entertainment Productions, SmartBot.net and Sanford Wallace. The FTC alleges the defendants used a variety of techniques to lure consumers to their Web sites, triggering installation of spyware programs.

These programs changed computers' home pages and search engines, created a storm of pop-up ads and caused the computers' CD-ROM trays to pop open. They also triggered pop-up ads for antispyware programs called Spy Wiper and Spy Deleter that would fix the newly created problems — for about $30.

Legislation pending

Shady spyware tactics have become so ubiquitous that the U.S. House of Representatives passed two antispyware bills in October 2004: 1) HR 2929, or the Spy Act, would require consumer consent for legal software that collects personal information from consumers, and 2) HR 4661, or the Internet Spyware Prevention Act of 2004, would establish criminal penalties for unauthorized access to computers.

Both bills are awaiting action in the Senate though the FTC claims neither is necessary. Existing deceptive practice laws and the technology solutions constantly being developed by major software manufacturers are enough to prosecute spyware vendors operating in the United States, according to the FTC.

FTC officials note that the CAN-SPAM Act signed into law in December 2003 has had little effect on e-mail-based spam, largely because many spammers operate outside U.S. borders. The same problem is likely to plague antispyware efforts.

Another potential stumbling block is defining spyware clearly enough for federal agencies to write rules implementing any laws that are passed. In the past, muddy language has made it impossible for regulators to determine what Congress intended in legislation.

Enforcement efforts continue

Regardless of whether new spyware laws are eventually passed or existing laws combined with education and technology become the weapons of choice, there is widespread agreement that something must be done about spyware.

The challenge for regulators is to keep the information superhighway free of potholes that could significantly rattle consumer confidence. As an FTC director said in announcing the complaints against Spy Wiper and Spy Deleter programs: "This is our first spyware case, but it won't be our last."

Crime doesn't have to pay

You can help prosecutors nab bankruptcy fraud perpetrators

According to the U.S. Trustee Program (a division of the U.S. Department of Justice), about 10% of bankruptcy cases involve some kind of fraud or other abuse. Criminal activities in bankruptcy can take many forms, as defined by Chapter 9 of Title 18 of the U.S. Code.

In some cases, business owners underreport assets or file false bankruptcy schedules. In others, they hide assets by transferring them to family members or to seemingly unaffiliated shell companies. With bust-outs, criminally minded entrepreneurs set up businesses for the exclusive purpose of bilking suppliers, lenders and customers before declaring bankruptcy.

Unearthing and prosecuting these crimes can be challenging. But with more than a million individuals and businesses now declaring bankruptcy every year, law enforcement is stepping up its efforts. In 1996, the Justice Department announced the launch of Operation Total Disclosure — a multiagency initiative designed to nab and prosecute those who would cheat creditors and consumers.

More recently, the U.S. Attorney's Office and the Office of the U.S. Trustee assembled a Bankruptcy Fraud Working Group to address enforcement issues and facilitate cooperation among the various agencies that investigate bankruptcy fraud.

Spotting bankruptcy crimes

Often, the first line of defense against bankruptcy fraud is its potential victims. If you believe a bankruptcy filed by one of your business customers is suspicious, consider engaging a forensic accountant to investigate. Forensic accountants can analyze the business's bankruptcy papers, financial statements and other public representations for irregularities.

If your forensic expert finds signs of fraud, he or she notifies the judge and trustee assigned to the case. These individuals then decide whether it warrants the attention of the U.S. Attorney's Office.

For the U.S. Attorney's Office, the most critical element of a bankruptcy crime is intent, or whether owners or executives acted in a willfully fraudulent manner. They base their decision to prosecute on, among other things, the size of the loss or injury and the quality of available evidence. In some cases, civil penalties are considered a sufficient alternative to criminal prosecution.

Indicting corporate criminals

Bankruptcy crimes are prosecuted when a U.S. Attorney files an indictment in federal district court. Federal prosecutors conduct an investigation and present their findings to a grand jury. If a majority of the members of the grand jury find probable cause to believe an offense has been committed, an indictment is returned and the case proceeds to trial.

While the process can be lengthy, federal prosecutors have had notable success, including the 2004 indictments of Jeffrey Skilling, former CEO of Enron, and Bernard Ebbers, former CEO of WorldCom.

Last October, the Justice Department announced, as part of Operation SILVER SCREEN, the indictments of 21 individuals in 17 different bankruptcy crime prosecutions. The offenses ranged from wire fraud to filing false statements, but the Justice Department estimates that, collectively, these cases represent the concealment of more than $7 million in assets.

Keep your eyes open

Even if you avoid doing business with new or other potentially risky companies, it's not always possible to avoid becoming a victim of bankruptcy fraud. But if one of your customers or business associates files for bankruptcy, don't hesitate to investigate; it may mean the difference between recovering some or all of what's owed you and nothing at all. Contact your regional U.S. Trustee Program office (www.doj.gov/ust) for more information.

Background checks can protect your business

Companies lose millions of dollars every year because they hire the wrong people for the job. While many employers are already familiar with the high cost of employee theft, they may be less aware of other, equally destructive employee behavior, such as filing false disability claims.

Bad apples can do more than eat into your company's budget; according to the U.S. Department of Commerce, 30% of businesses go under mainly because of poor hiring practices. Clearly, performing background checks on job candidates should be an essential part of your hiring process.

Cost of crooked employees

Background checks can reveal many things — resumé inaccuracies, a history of job hopping, litigious behavior and even criminal charges — all of which could eventually affect your business.

A sample study of 300,000 background checks conducted by background screening company USA-FACT found that 5% of applicants had criminal records, 36% had motor vehicle violations, 18% had prior employment that could not be verified and 11% had education credentials that were not legitimate.

Given these numbers, you'd be remiss not to perform at least a basic screening. Employers must, at the very least, verify employees' work eligibility status, in compliance with immigration laws. And if you're hiring in certain fields, such as law enforcement, security, trucking, child care and elder care, you must perform criminal background checks on all potential hires.

Optional yet valuable

While optional, you should, nevertheless, always verify an applicant's previous employment — including contacting all references — to ensure the person actually held the positions he claims or that her former managers were satisfied with her job performance. And confirm that applicants have the academic credentials, military service record and professional licenses stated on their resumés.

Many employers also run credit report checks on potential employees. Credit reports can reveal whether the candidate is consistently late in paying bills, is swimming in debt or has filed for bankruptcy — important information to have if you're hiring someone to work with money or for another position of fiscal responsibility. And if you'll be providing your new hire with a company car, first check that individual's driving record.

While you certainly have the right to know if a new hire is going to harm your business, keep in mind that employees' privacy and other rights are protected by federal law.

The Fair Credit Reporting Act (FCRA) requires that employers obtain signed employee agreements before they request any type of "consumer report" — which covers credit reports, criminal background checks and many other types of information gathering. For a full list of the rules, visit the Federal Trade Commission's Web site at www.ftc.gov.

Getting outside help

Since it's not always easy or time-efficient to collect background information yourself, background screening services, with their teams of researchers and instant access to public databases, are a potential solution.

If you type "background checks" into any Internet search engine, dozens of screening agency sites pop up. But knowing which firm boasts a good reputation and reasonable fees isn't as simple as choosing the first name on Google's search result list. In fact, the best way to find a screening firm is through

word-of-mouth — from other business owners or human resources managers.

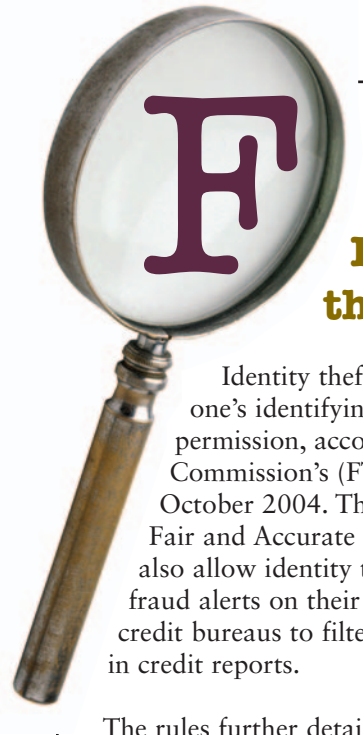
The agency you choose should demonstrate compliance with FCRA regulations and any applicable state laws. It should also inform you of your obligations and your employee's rights and provide you with all the necessary consent forms.

The cost of screening services varies, depending on the scope of the job. Services beyond a basic screening — such as searching public records in several different counties or states — will cost extra.

Most online services can verify an applicant's identity within minutes and other background information within 48 to 72 hours.

Better safe than sorry

While background checks require a little time and money, most employers find they're worth their weight in gold. Simply knowing you perform background checks will discourage most dishonest job applicants and promote a more ethical work environment for all of your employees.



Fraud to watch for:

FTC rules define, clarify identity theft procedures

Identity theft is defined as using someone's identifying information without permission, according to the Federal Trade Commission's (FTC) final rules issued in October 2004. The rules, issued under the Fair and Accurate Credit Transactions Act, also allow identity theft victims to place fraud alerts on their credit files and ask credit bureaus to filter or alter information in credit reports.

The rules further detail the proof of identity required to implement these actions, and provide for 12-month alerts in the credit files of military personnel who are deployed. The latter may be extended if military deployments last longer than a year.

Victims' rights

In conjunction with the final rules, which took effect Jan. 31, 2005, the FTC supplied documents that summarize identity theft victims' rights. They also detail responsibilities of consumer reporting agencies and the organizations that furnish information to those agencies.

Consumers who have been the victims of identity theft must use "identity theft reports" to place extended fraud alerts on their credit files or to keep information obtained through identity theft from appearing in those files. They also may ask that credit reports contain a truncated version of their Social Security numbers.

At the same time, however, the FTC recognized that consumers could misuse such reports to block legitimate negative information. Therefore, credit bureaus and creditors may request additional information from consumers to establish that identity theft did indeed occur.

Matching mechanisms

Finally, credit reporting agencies must develop mechanisms to ensure that all consumers and their files are appropriately matched.

The FTC has stopped short of mandating those mechanisms, but has suggested files include consumers' full names, addresses, and Social Security numbers or birthdates, along with copies of utility bills and a government-issued identification or questions to which only the consumer would know the answers.

Copies of the final rules can be found on the FTC Web site at www.ftc.gov.

Craig L. Greene, CFE, CPA

An internationally recognized public speaker, Craig has lectured on topics involving fraud and its detection to auditors, investigators and attorneys. He is a faculty member of the Association of Certified Fraud Examiners and Institute of Internal Auditors.

Craig works as a consultant and expert witness for major corporations, law firms, law enforcement and governmental agencies on cases involving allegations of fraud and misrepresentation. Craig is frequently quoted in major newspapers and publications throughout the U.S.

McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

Specialists in Fraud Examination and Litigation Services

If a business hasn't yet been a victim of fraud, it's been fortunate. According to the Association of Certified Fraud Examiners, fraud costs businesses in the United States billions of dollars every year. Small businesses are especially vulnerable because they often do not have controls in place to reduce the likelihood of fraud.

This is where McGovern & Greene LLP can help. Our firm specializes in helping corporations, attorneys, lenders, law enforcement and governmental agencies analyze financial records and contracts, identify and prevent fraud, recover and analyze evidence, and provide expert testimony in all of these matters. Our highly-experienced team of professionals includes certified fraud examiners and certified public accountants that are experts in the fields of fraud examination, forensic accounting, computer forensics, damage calculations, business valuations and audit services.

Our professionals can assist you in a wide range of matters, including:

- Fraud Examination
- Financial Investigations
- Forensic Accounting
- Asset Recovery
- Internal Audit Services
- Computer Forensics
- Training & Seminars
- Healthcare Audit
- Business Valuation
- Litigation Services
- Government Contracts
- Economic Damages
- Intellectual Property
- Contract Claims
- Construction Audits
- Electronic Discovery
- Profit Recovery
- Due Diligence

We welcome the opportunity to discuss your needs and answer any questions you might have about our fraud examination and litigation services.

Please contact us at 312.419.1961 or visit us at www.mcgoverngreene.com and let us know how we can be of assistance.

McGovern & Greene LLP
105 W. Madison Street, Suite 406
Chicago, Illinois 60602