

BANK

MANHAM CITY BANK  
14501 Sweitzer Lane • Laurel, ME • 20707-5902 • (301) 206-WSSC (9772) • (301) 206-8345  
FAX (301) 206-8114 • TTY (301) 206-8345  
Interactive Voice Response System (IVRS) • Available 24 hours a day.

MANHAM CITY BANK

CHECK CARD

DEBIT

4244 0404 2620 9843

06/05 05/08

WATER AND SEWER BILL

Service Address  
3009 Nill Lane

Previous Balance...  
Payment(s) Received 04/19/05...  
We thank you for your payment

152

65-7198/2550

Kent Gray  
3009 Nill Lane  
Manham, ME 27706

Pay to the  
Order of

Dollars

# Civil liability for identity theft

JEFFREY R. DION AND JAMES A. FERGUSON

*Identity theft can cause catastrophic financial damage, but many victims also suffer emotional, psychological, and even physical injuries. Civil claims against the responsible parties can help repair the damage.*

The crime of identity theft is widespread. While the incidence of some form of identity theft declined to 8.9 million Americans in 2005<sup>1</sup> from almost 10 million Americans in 2002,<sup>2</sup> it remains a significant problem for those victimized.

The average out-of-pocket loss from identity theft is about \$6,000,<sup>3</sup> though many victims lose even more in terms of time and emotional health. The average victim, for example, spends 40 hours trying to repair his or her credit.<sup>4</sup>

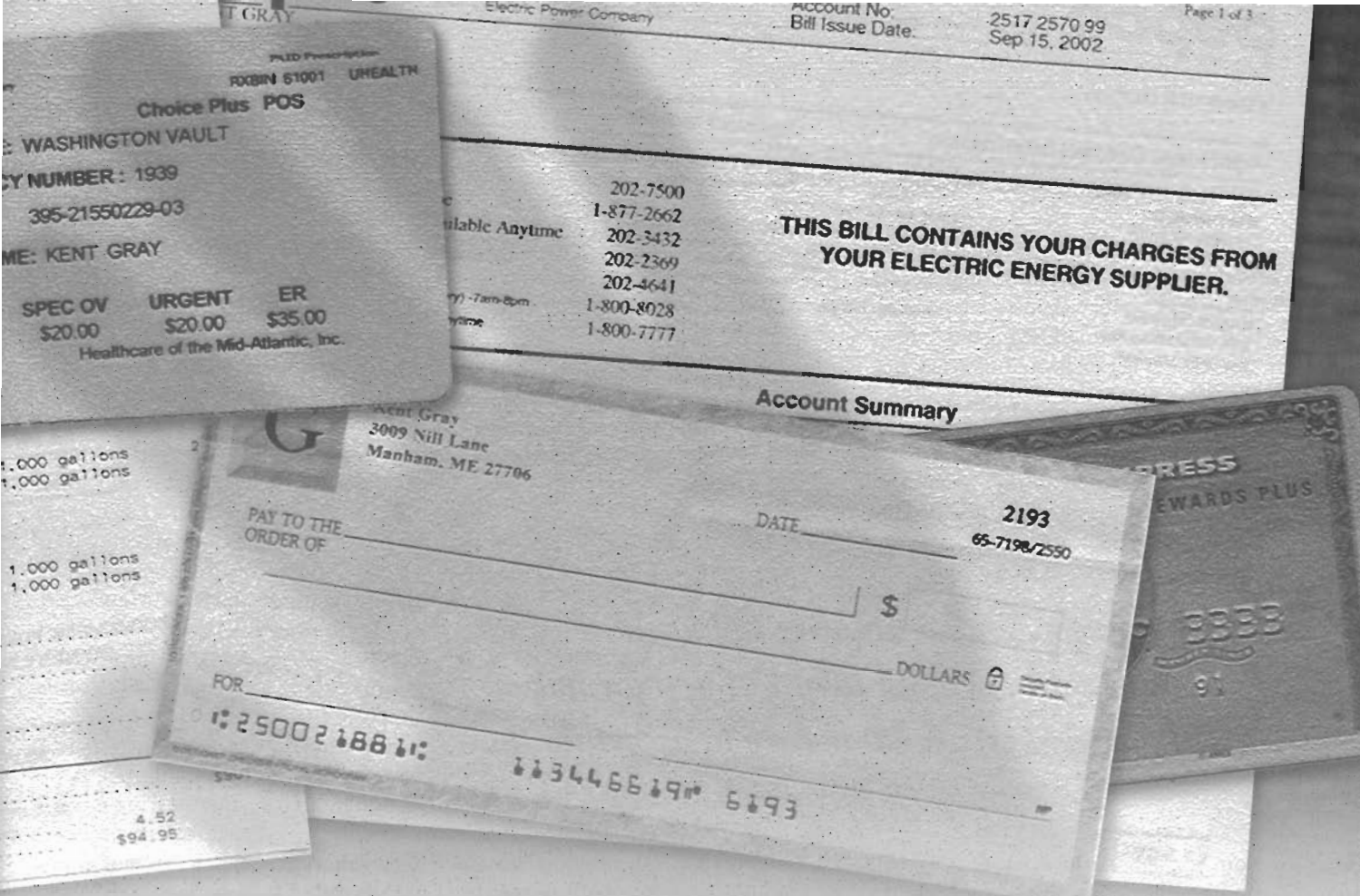
Recovering from a stolen identity isn't easy, but victims are not without recourse. Both criminal and civil law provide ways for victims to gain restitution for their losses and seek justice against the perpetrator or responsible third parties.

A wide variety of criminal acts fall under the heading of identity theft. Generally, it involves the unauthorized use of a person's identifying information (such

as his or her name, date of birth, or Social Security number) to steal money or services, commit fraud, or engage in other illegal activities. More than 40 percent of identity thefts involve credit card fraud, but thieves also target bank accounts, telephone or utility accounts, government benefits, and a host of other financial transactions.

On average, more than a year passes between the first misuse of a person's identity and the time he or she discovers the crime. Once this happens, the person should take certain steps right away. The Federal Trade Commission (FTC) recommends that victims quickly contact the fraud department of any one of the three major credit reporting agencies to have fraud alerts placed on their credit files.<sup>5</sup> They should immediately close any accounts that have been affected.

The crime should also be reported to the police as soon as possible. Almost



every state has a law specifically criminalizing identity theft, and a growing number of states have laws allowing victims to have a temporary security hold placed on their credit report by credit reporting agencies to prevent further damage. In addition, the 1998 Identity Theft and Assumption Deterrence Act made identity theft a federal crime.<sup>6</sup>

A successful criminal prosecution may result in an order of restitution compelling the perpetrator to pay the victim for losses caused by the identity theft. Although restitution may fully compensate some victims, others may want to pursue a civil lawsuit.

An identity theft victim can sue the perpetrator of the crime, seeking compensation for both economic damages and noneconomic damages, such as pain and suffering. Depending on the facts, the suit might invoke various common law causes of action, including misrep-

resentation, fraud, or conversion.

Several states, including California,<sup>7</sup> Connecticut,<sup>8</sup> Iowa,<sup>9</sup> Louisiana,<sup>10</sup> New Jersey,<sup>11</sup> and Pennsylvania,<sup>12</sup> have enacted statutes that create a civil cause of action for identity theft, some of which allow victims to recover treble damages and attorney fees.

In addition to the perpetrator, other parties may be liable for the harms suffered by an identity theft victim. Third-party liability claims fall into four general categories: negligent security of personal information, negligent sale of information, failure of a bank to prevent identity theft or to mitigate damages, and liability of credit reporting agencies for failure to prevent or remedy incidents of fraud.

Claims for negligent security of personal information are based on the theory that accurate personal identifying information is the key that allows access

to a person's financial accounts and credit. Parties who maintain such information in the normal course of business have a legal duty to reasonably safeguard that information from being used for an illegitimate purpose.

These claims are analogous to a premises liability claim for negligent security resulting in a violent criminal assault. In both cases, the defendant is alleged to have failed to take reasonable precautions to protect the victim from foreseeable injuries caused by a third party.

Interestingly, some courts have applied broader duties to protect people

JEFFREY R. DION is the director of the National Crime Victim Bar Association. He can be reached by e-mail at [jdion@ncvc.org](mailto:jdion@ncvc.org). JAMES A. FERGUSON is the executive director of Legal Services of Northern Virginia. He can be reached at [jferguson@lsnv.org](mailto:jferguson@lsnv.org).

from identity theft than to protect them from physical harm.

For example, in *Bell v. Michigan Council 25 A.F.S.C.M.E.*, the Michigan Court of Appeals, in an unpublished opinion, upheld a jury verdict against a labor union that was sued for failing to properly secure its members' personal information.<sup>13</sup> The 12 plaintiffs were 911 operators for the city of Detroit whose membership in the union was essentially mandatory.

The city provided the union treasurer with a quarterly report that included important personal information about each employee, such as job classifica-

tion of [proximate cause] is a difficult one. But we believe that these factors must be considered in light of the technological age in which we now live. Even as recent as a decade ago, it could be said that the likelihood of identity theft occurring as the result of personal information being allowed to leave [the] defendant's premises was remote. However, today, the possibility of identity theft is all too commonplace. Under the circumstances of this case, we find that there is a strong basis for concluding that the criminal acts were foreseeable in this case.<sup>14</sup>

Evidence of damages in an identity theft case is often problematic. However,

## *Courts have extended liability to businesses that have sold personal identifying information without using reasonable care to ascertain the purpose for which it was sought.*

tion, Social Security number, and pension number. The treasurer's daughter was convicted of appropriating the 911 operators' identities to purchase goods and secure phone service in their names.

Michigan does not recognize a duty to protect against the acts of a third party absent a special relationship. The *Bell* court found that there was a special relationship between the union and its members and that the union had a legal obligation to act on behalf of and in the best interests of its members.

It also held that the misuse of the members' personal information was foreseeable because the union knew the treasurer took the information home. The union allowed this practice to continue, despite repeated objections by members of its executive board.

The court took notice of the increasing threat of identity theft and found that a jury could expect the union to recognize it as well:

While no organization can 100 percent prevent illegal activities of third parties, it can certainly decrease the likelihood, as in this case, by not providing easy access to such sensitive information. The evidence showed that the union had absolutely no procedures or safeguards in place to ensure that confidential information was not accessed by unauthorized persons. The ques-

tion of [proximate cause] is a difficult one. But we believe that these factors must be considered in light of the technological age in which we now live. Even as recent as a decade ago, it could be said that the likelihood of identity theft occurring as the result of personal information being allowed to leave [the] defendant's premises was remote. However, today, the possibility of identity theft is all too commonplace. Under the circumstances of this case, we find that there is a strong basis for concluding that the criminal acts were foreseeable in this case.<sup>14</sup>

Evidence of damages in an identity theft case is often problematic. However,

the *Bell* court found that testimony by the 12 plaintiffs that each had spent many hours trying to correct the problems caused by the identity theft—coupled with concrete examples of their aggravation, anguish, and humiliation at being denied credit—supported the jury's damages award.

### **Negligent sale of information**

Courts have also extended liability to businesses that have sold personal identifying information without using reasonable care to ascertain the purpose for which it was sought. *Remsburg v. Docusearch, Inc.*, a stalking and homicide case, has direct implications for identity theft claims.<sup>15</sup>

Liam Youens maintained a Web site on which he detailed his obsession with, and his intent to kill, Amy Boyer. Using an online investigation site called Docusearch.com, Youens obtained personal information about Boyer. In five separate transactions during a six-week period, Youens paid Docusearch a total of \$204 to obtain her date of birth, Social Security number, place of employment, and home address. He went to Boyer's workplace, shot and killed her as she was leaving her office, and then shot

and killed himself.

Boyer's estate sued Docusearch in federal court, which certified a question to the New Hampshire Supreme Court, asking it to determine whether the company could be held liable for Boyer's death under various applications of state law. The high court found that it could.

The court first observed that everyone has a legal duty to exercise reasonable care not to subject others to an unreasonable risk of harm. This duty arises when the risk is sufficiently foreseeable. In Boyer's case, the court said, the risk of criminal misconduct arising from stalking and identity theft is sufficiently foreseeable that an investigative service has a duty to act with reasonable care when disclosing a third party's personal information to a client.

The court also ruled that a person whose Social Security number is obtained by an investigator from a credit reporting agency without the person's permission may have a cause of action for the tort of intrusion upon seclusion. For the claim to succeed, the court said, the plaintiff must prove that the intrusion would have been offensive to a person of ordinary sensibilities.<sup>16</sup>

Finally, the court found that Docusearch's use of false-pretense phone calls to obtain Boyer's information violated New Hampshire's Consumer Protection Act, which could make Docusearch liable for damages.<sup>17</sup>

### **Failure to act**

Some identity theft victims have sought to sue banks for failing to take reasonable steps to protect customers after learning that fraudulent accounts were opened in the customers' names. *Murray v. Bank of America, N.A.*, highlights the duty of a bank to prevent further damages once it is on notice that an account is fraudulent.<sup>18</sup>

Margaret Murray lost her driver's license in May 1997. Later that month, a woman opened a Bank of America account in Murray's name and wrote 60 fraudulent checks from the account totaling about \$7,500.

On June 2, 1997, Murray went to the bank and discovered the fraudulent account. She demanded that bank em-

employees close the account and asked them to inform the merchants who had received the bad checks that she was innocent and that the account was fraudulent. Murray also reported the fraudulent account to the police.

A month passed before the bank finally closed the account, and no merchant was informed of Murray's innocence. In November 1997, Murray was arrested and charged with bank fraud. She spent 12 hours in jail before being released on bond. She then obtained a letter from the bank stating she was not the person who opened the account.

The damages suffered by the plaintiff in *Patrick v. Union State Bank* were even more severe than those Murray suffered.<sup>20</sup> After fraudulent checks were written in her name to draw money from an account at the Union State Bank, Bridgette Patrick was charged with issuing worthless checks and jailed for 10 days. She then had to make several court appearances in various jurisdictions. All the charges against her were eventually dismissed.

Patrick sued the bank, alleging that it had negligently allowed an unknown woman, fraudulently posing as Patrick, to

glas Reid dba Bear Stearns." The Wachovia employee who opened Reid's account did not verify that Reid was authorized to operate under the name Bear Stearns. Reid had no such authority and was not affiliated with Bear Stearns.

Eisenberg sued Wachovia, alleging that the bank had negligently allowed Reid to establish and operate a fraudulent account and negligently failed to train its employees to detect fraud. The trial court granted Wachovia's motion to dismiss the complaint on the ground that both negligence claims were preempted by Federal Reserve Board regulations.

The Fourth Circuit Court of Appeals, in a de novo review, found that the regulations did not preempt the negligence claims.<sup>22</sup> However, the court ruled that the claims still failed because the bank had owed Eisenberg no duty of care given the facts of the case.<sup>23</sup>

## *Credit reporting agencies can be held liable under the Fair Credit Reporting Act for negligently releasing credit information or failing to correct fraudulent information on a credit report.*

Murray, who was required to appear at three criminal court hearings, was exonerated of all charges. However, she began suffering physical manifestations brought on by stress and anxiety from the experience. She sued the bank for negligence, and a jury awarded her damages. The bank appealed.

The South Carolina Court of Appeals affirmed the verdict. The court held that the bank owed Murray a duty of care and that the issue of whether the bank breached that duty was properly submitted to the jury. Noting that the bank had failed to follow its own procedures, close the account promptly, and notify any merchants that the account was fraudulent, the court concluded that there was sufficient evidence from which the jury could find that the bank had breached its duty to Murray.<sup>19</sup>

The court also dismissed the bank's claim that the damages were excessive, finding that Murray suffered humiliation and physical duress as a result of her arrest. Because she was arrested in front of her neighbors, her acute embarrassment compelled her to move and incur other expenses. She also suffered stress-related physical illnesses. Based on these factors, the court concluded, the amount of the jury's award did not shock the conscience.

open a checking account and that it had failed to demand proper identification and to verify information that was obtained at the time the account was opened. The trial court granted summary judgment for the bank, finding that there were no material facts in dispute and that Patrick had not established the action's elements of duty and proximate cause.

On appeal, the Alabama Supreme Court held that a bank owes a duty of reasonable care to a person in whose name, and on whose identification, an account has been opened to ensure that the person opening the account is not an imposter. The court said it was a question of fact whether the imposter's fraudulent acts were foreseeable, precluding summary judgment for the bank.<sup>21</sup>

While some plaintiffs have succeeded in holding banks liable when fraudulent accounts were opened in their name, others have hit roadblocks when they sued after being duped into depositing funds into a fraudulent account.

For example, in *Eisenberg v. Wachovia Bank, N.A.*, Douglas Reid falsely represented to Eric Eisenberg that he was a vice president with Bear Stearns Securities. Reid convinced Eisenberg to deposit \$1 million by electronic wire into a Wachovia account bearing the name "Dou-

### **Liability of credit reporting agencies**

Credit reporting agencies can be held liable under the Fair Credit Reporting Act (FCRA) for negligently releasing credit information or failing to correct fraudulent information on a credit report.<sup>24</sup> In the case of *TRW v. Andrews*, Adelaide Andrews visited a doctor's office and filled out a form listing her name, address, Social Security number, and other personal information.<sup>25</sup> An office receptionist named Andrea Andrews (the identity thief) copied the data and attempted to obtain credit from various companies using Adelaide's Social Security number but her own name and address. TRW released credit information to the companies, which Andrea used to get credit.

After Adelaide discovered the fraud, she sued TRW for violations of the FCRA. Although the trial court found that her claims were time-barred, the Ninth Circuit Court of Appeals reversed, holding that the FCRA's statute of limitations begins to run when the victim discovers the fraud. TRW appealed to the U.S. Supreme Court, which held that the limitations period began to run when the cause of action accrued—that is, when TRW improperly transmitted the credit report, rather than when Adelaide discovered the FCRA violation.

In response to the Supreme Court's ruling, Congress amended the FCRA to make it easier for victims of identity theft to sue credit reporting agencies after they discover latent identity theft problems. A claim must now be brought within two years of the discovery of a violation, or five years from the date of the violation, whichever is earlier.<sup>26</sup>

A significant component of damages in cases of identity theft is the degrading of the victim's credit rating as a result of adverse information in the victim's credit report caused by fraudulent activity. These damages are exacerbated when credit reporting agencies fail to correct the information or identify allegations of fraud.

In *Kirkpatrick v. Equifax*, an identity theft victim learned that multiple lines of credit had been fraudulently established in his name and that his credit rating had been ruined.<sup>27</sup> The victim contacted Equifax and asked it to clear his credit history. He provided a police report and affidavit to support his claim.

Despite his repeated efforts, Equifax took no action to correct his credit record. He sued Equifax under the FCRA, alleging emotional distress due to repeated denials of credit, and a jury awarded him damages and attorney fees.

Civil liability for identity theft is a rapidly evolving area of the law, and there are significant hurdles to recovery that could stand in a victim's way. Despite such challenges, identity theft victims and their attorneys should keep in mind that civil lawsuits may provide meaningful compensation for the losses victims have suffered. ■

#### Notes

1. Council of Better Business Bureaus, Inc., *New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think*, <https://secure.platypusvideo.com/articlenews/article.php?articleID=25> (last accessed Nov. 22, 2006).

2. Synovate, *Federal Trade Commission—Identity Theft Survey Report 4* (Federal Trade Commission Sept. 2003), [www.ftc.gov/os/2003/09/synovaterreport.pdf](http://www.ftc.gov/os/2003/09/synovaterreport.pdf) (last accessed Nov. 22, 2006).

3. *Id.* at 6-7.

4. Rubina Johannes, *2006 Identity Fraud Survey Report* (abridged) (Javelin Strategy Research Jan. 2006), [www.javelinstrategy.com/products/99DEBA/27/delivery.pdf](http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf) (last accessed Nov. 29, 2006).

5. The three major credit bureaus are Equifax ([www.equifax.com](http://www.equifax.com)), Experian ([www.experian.com](http://www.experian.com)), and TransUnion ([www.transunion.com](http://www.transunion.com)).

6. 18 U.S.C. §1001 (2006).

7. Cal. Civ. Code §1798.93 (West 2006).

8. Conn. Gen. Stat. §52-57h (2006).

9. Iowa Code §714.16B (2005).

10. La. Stat. Ann. §9:3568 (2006).

11. N.J. Stat. Ann. §56:11-50 (West 2005).

12. 42 Pa. Consol. Stat. Ann. §8315 (2006).

13. 2005 WL 356306 (Mich. App. Feb. 15, 2005), *appeal denied*, 707 N.W.2d 597 (Mich. 2005).

14. *Id.* at \*5.

15. 816 A.2d 1001 (N.H. 2003).

16. *Id.* at 1008.

17. N.H. Rev. Stat. Ann. §358-A:2 (West 2006).

18. 580 S.E.2d 194 (S.C. App. 2003).

19. *Id.* at 198.

20. 681 So. 2d 1364 (Ala. 1996).

21. *Id.* at 1371.

22. 301 F.3d 220 (4th Cir. 2002).

23. *Id.* at 223.

24. 15 U.S.C. §§1681-1681x (2006).

25. 534 U.S. 19 (2001).

26. 15 U.S.C. §1681p (2006).

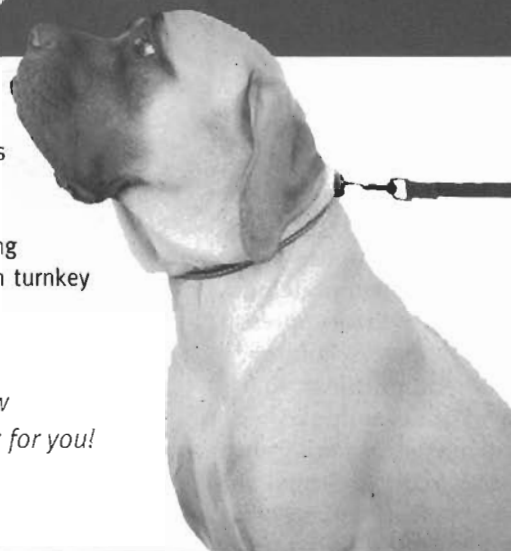
27. 2005 WL 1231485 (D. Or. Jan 25, 2005).

## Unleash Your Productivity Potential

**Increase your caseload** through the efficiency of TrialWorks Case Management Software. From sole practitioners to large firms, TrialWorks is the case management software that fits your needs and will even teach you a new trick or two.

Trialworks and EMSI have partnered to provide integrated ordering of medical records through the Trialworks' system. **EMSI** specializes in turnkey medical records retrieval services that deliver complete, efficient, and cost effective solutions no matter what your needs.

Contact us today for a free online demo and see how  
**TrialWorks** will work for you!



800.377.5844 [www.TrialWorks.com](http://www.TrialWorks.com)