

Journal of  
**Health Care  
Compliance**

Balance

Guidelines

**Augmented Informed Consent Helps  
Health Care Organizations Respond to  
New JCAHO Survey Tactics**

**Medical Identity Theft: The Future Threat  
of Health Care Fraud Is Now**

**Teleradiology: Compliance Concerns  
and Solutions, Part 1**

**Economic Credentialing: An Examination  
and Critique of HHS' View of Conflict  
Credentialing**

Effectiveness

# Medical Identity Theft: The Future Threat of Health Care Fraud Is Now

Lack of Federal Law Enforcement Efforts Means  
Compliance Professionals Will Have to Lead the Way

Latour "LT" Lafferty

Are you concerned about the future threat of identity theft in your health care organization as you transition to an electronic health care records system? Since 1992, there have been 19,428 complaints to the Federal Trade Commission (FTC) about medical identity theft, and the nonprofit public interest research group World Privacy Forum (WPF) estimates that medical identity theft has victimized as many as a half million people.<sup>1</sup> Pam Dixon, the executive director of the WPF and "the leading authority" on medical identity theft, believes "that future [threat] is now."<sup>2</sup>

Medical identity theft has been described as the "newest frontier in the ever-evolving crime of identity theft"<sup>3</sup> and presents a ripe opportunity for a variety of perpetrators as the health care industry evolves into an electronic culture. This environment, however, is not adequately protected by current law enforcement agencies and criminal offenses.

As a result, medical identity theft presents a widespread threat in the health care industry, but there exists little deterrent threat from the threat of prosecution. Accordingly, health care compliance professionals must lead the way in the effort to combat the future threat of health care fraud through medical identity theft.

## **A. FINANCIAL VERSUS MEDICAL IDENTITY THEFT**

There is a critical distinction between *financial* identity theft and *medical* identity theft, which is the fact that the "hallmark" of medical identity theft is the falsification of the victim's medical record with information from the perpetrator and crime.<sup>4</sup> First, however, con-

Latour "LT" Lafferty is a shareholder with Fowler White Boggs Banker in Tampa, Florida and practices in the firm's White Collar Crime & Government Investigations Group. Mr. Lafferty is a former criminal and civil federal prosecutor having served 10 years as an Assistant U.S. Attorney (AUSA) in the Middle District of Florida. Mr. Lafferty is certified by the Health Care Compliance Association (HCCA) in Healthcare Compliance (CHC) and has published numerous articles and regularly speaks on Healthcare Corporate Compliance and Trial Advocacy topics. He can be reached at [ltlafferty@fowlerwhite.com](mailto:ltlafferty@fowlerwhite.com).

sider that financial identity theft is on the rise and ranks as one of the top consumer fraud complaints in the nation according to the FTC.<sup>5</sup>

Financial identity theft is characterized as a crime of opportunity<sup>6</sup> and occurs anytime someone misappropriates your name, social security number, or other personal information to commit fraud or other crimes.<sup>7</sup> Victims are targeted simply because their information is available (*i.e.*, they are easy targets). The federal Identity Theft and Assumption Deterrence Act (Act) and many state statutes (*e.g.*, Florida Statutes § 817.568) criminalize identity theft.<sup>8</sup> The Act also established the FTC's identity theft program, which includes the core initiatives of assisting victims, educating consumers, law enforcement, and businesses, and established an identity theft data clearinghouse for the maintenance and dissemination of information.<sup>9</sup>

In 2003, the FTC published its identity theft survey report finding that in the previous five-year period approximately 10 million American consumers discovered that their personal information had been used to open fraudulent bank, credit card, or utility accounts or used to commit other crimes.<sup>10</sup> The FTC estimated that the total loss to victims for identity theft was almost \$53 billion dollars annually and that Americans spent 300 million hours resolving issues related to identity theft.<sup>11</sup>

Amazingly, the FTC found that in over 25 percent of reported identity theft cases, the victims knew or were related to the identity thief and that most cases originated in the workplace.<sup>12</sup> The survey found that approximately 70 percent of identity theft cases are committed by a co-worker, employee, or business owner (*i.e.*, insiders).<sup>13</sup>

Second, consider that *medical* identity theft is on the rise because of the increasingly high costs of health care services.<sup>14</sup> Total health expenditures in the United States are estimated to be \$2.16 trillion in 2006 and are projected to rise to over \$4 trillion in 2015.<sup>15</sup> It also is estimated that

health care fraud accounts for up to 10 percent of these expenditures.<sup>16</sup>

Consequently, Congress created the health care fraud and abuse program when it enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996.<sup>17</sup> This highly coordinated national law enforcement effort is intended to ensure the integrity of federally subsidized health care benefits and resulted in 537 criminal prosecutions, 3,806 program exclusions, and 250 civil enforcement actions resulting in savings and expected recoveries of \$35.4 billion for fiscal year 2005.<sup>18</sup>

From this perspective, it is easy to understand why fraudsters will "set their sights" on health care providers — "because that is where the money is."<sup>19</sup> Quite simply, "medical identity theft is the newest frontier in the ever-evolving crime of identity theft"<sup>20</sup> and grew by 197 percent from 2001 to 2005 according to the FTC.<sup>21</sup>

In the context of health care, *medical* identity theft may be viewed as a subset of both health care fraud and identity theft<sup>22</sup> and has been characterized as combining "an unwholesome criminal trilogy of medical privacy violations, identity theft, and health care fraud."<sup>23</sup> Medical identity theft — in contrast to financial identity theft — occurs anytime a person's identity, such as his or her name or insurance information, is misappropriated to obtain medical services or goods or to make false claims for medical services or goods and falsify medical records to support those claims.<sup>24</sup>

Identity theft may occur in a medical setting but not constitute medical identity theft, such as when a health care employee steals a patient's credit card and makes illegal purchases.<sup>25</sup> Further, health care fraud may involve the falsification of medical records and not involve identity theft, such as when a physician alters a medical record to cover up a medical error.<sup>26</sup> Neither of these cases, however, captures the true essence of medical identity theft, which is the theft of a person's *medical identity*.

