Volume XII, Number 6 Monday, April 18, 2005

**Expanded Issue**


*From the Desk of R. Lewis Dark...*

# THE DARK REPORT

**RELIABLE BUSINESS INTELLIGENCE, EXCLUSIVELY FOR MEDICAL LAB CEOs / COOs / CFOs / PATHOLOGISTs**



**Restricted information, see page 2**

Commentary & Opinion by...

R. Lewis Dark

Founder & Publisher

## *More Crime, More Consolidation, and a New Threat*

IT'S A SHAME THAT OUR LEAD STORY IN THIS ISSUE IS CRIMINAL INDICTMENTS of six former **IMPATH** executives. It is a black mark on the lab industry and is just one more factor that makes it tougher for honest laboratorians to successfully lobby Congress on adequate funding for laboratory testing services.

Our follow-up story to crime at IMPATH is news of the just-announced sale of **Esoterix, Inc.** to **Laboratory Corporation of America**. It's another example of further consolidation within the laboratory industry. When Esoterix is bought by LabCorp sometime in the next ten weeks, it will remove another independent competitor from the national lab services marketplace.

Once you get past those two stories, you will find a detailed interview with Eric Drew. He's the cancer patient, near death, whose identity was ripped off by a phlebotomist in the hospital where he was being treated. Discovery of the crime launched Drew into an extraordinary investigation which culminated in the conviction of this nefarious lab worker under the HIPAA (Health Insurance Portability and Accountability Act) statute. It was the first-ever federal conviction of a HIPAA crime.

Drew's story is exclusive to THE DARK REPORT. We have extensively researched these events for an important reason: lab managers and pathologists need to know how vulnerable their laboratory or pathology group practice is to the crime of patient identity theft. During the course of his interview with THE DARK REPORT, Drew explains, for the first time, many new details of how his identity was stolen. He also discusses the "do nothing" attitude of the hospital's privacy and compliance people when he first alerted them to the crime and requested their help to identify the perpetrator and bring him to justice.

I was shocked when I read Eric Drew's story. I believe the majority of you will also be shocked. I use the word "shock" deliberately. From the hospital to the police, the system failed Eric Drew—utterly and totally. My common sense tells me that the majority of labs and pathology group practices would do the right thing were a patient to show up and declare his/her identity was stolen and he/she has good reason to believe it occurred in the lab. But then again, do you have equal confidence that the privacy officer in your lab would acknowledge the possibility of a crime and support this patient in the search for truth—regardless of where it may lead your laboratory? TDR

# Ex-IMPATH Executives Face Criminal Charges

## *Federal government files various charges against six former IMPATH executives*

***CEO SUMMARY: With the announcement by Federal prosecutors of criminal and civil actions against a total of seven ex-IMPATH executives, IMPATH becomes the laboratory industry's worst criminal scandal. Federal prosecutors contend these executives, during their employment at IMPATH, engineered an accounting fraud that resulted in manufacturing as much as $64 million in non-existent revenue.***

SIX FORMER EXECUTIVES of **IMPATH, Inc.** were charged by federal prosecutors of conspiracy, securities fraud, and other criminal charges. The case was announced on Wednesday, March 30, 2005 by David N. Kelly, United States Attorney for the Southern District of New York.

Federal prosecutors say these ex-IMPATH executives manipulated the company's finances to produce as much as $64 million in "phantom revenue." The activity described in the indictment occurred between 1999 and 2002.

Not until July 2003 was the fraud, and its magnitude, discovered. By then, Saad and Adelson were no longer employed by IMPATH. Company officials broke the news on July 30, 2003, stating that an internal investigation was uncovering "possible accounting irregularities," of which the most significant was a material overstatement of revenues.

This announcement triggered a drop in the company's stock price of 88%. Losses to investors approached $260 million. NASDAQ delisted the company. On September 29, 2003, IMPATH filed a Chapter 11 bankruptcy action. *(See TDR, September 29, 2003.)*

Topping the list of those indicted were former Chairman and CEO Anu Saad, Ph.D. and former President and COO Richard P. Adelson. Saad is facing charges that include one count of conspiracy, one count of securities fraud, two counts of soliciting proxies with false proxy statements, and two counts of making false filings with the **Securities and Exchange Commission** (SEC).



THE DARK REPORT Intelligence Briefings for Laboratory CEOs, COOs, CFOs, and Pathologists are sent 17 times per year by The Dark Group, Inc., 21806 Briarcliff Drive, Spicewood, Texas, 78669, Voice 1.800.560.6363, Fax 512.264.0969. **(ISSN 1097-2919.)**

R. Lewis Dark, Founder & Publisher. Robert L. Michel, Editor.

SUBSCRIPTION TO THE DARK REPORT INTELLIGENCE SERVICE, which includes THE DARK REPORT plus timely briefings and private teleconferences, is $11.90 per week in the US, $12.50 per week in Canada, $13.65 per week elsewhere (billed semi-annually).

Charges against Adelson are one count each of conspiracy and securities fraud and eight counts of making false filings with the SEC. Saad faces a maximum penalty of 65 years in prison and fines of $15.25 million (twice the gain or loss resulting from the crime). Adelson's charges carry a maximum penalty of 45 years of prison time and fines of $10.25 million (also twice the gain or loss from the crime).

## Already Four Guilty Pleas

Four executives charged in this case have already pled guilty. They are David J. Cammarata (former Chief Financial Officer), Peter Torres (former Vice President of Finance), Karin Gardner (former Controller), and Kenneth Jugan (former National Billing Director).

In addition to the criminal counts, the SEC filed civil charges against all six, plus one other individual. Former IMPATH Vice President Robert McKie, without admitting or denying SEC allegations, agreed to settle his case by paying a $150,000 penalty and returning about $100,000 in bonuses, with interest.

Of passing interest is the fact that the company which previously audited IMPATH's books was not charged or fined. **KPMG LLP** seems to have dodged all the legal bullets in this case.

## Other Legal Liability

While in bankruptcy, IMPATH was purchased by **Genzyme Corporation** in early 2004. Federal prosecutors have declined to comment on whether Genzyme faces any type of legal liability as a consequence of its purchase of specific parts of IMPATH's business. (IMPATH's **Cancer Registry** and **Tamtron** business units were sold to **IMPAC Medical Systems, Inc.** in December 2003.)

It must be noted that both the federal indictments and the SEC civil charges describe illegal activity that does not include violation of Medicare and Medicaid statutes. The legal actions initiated against these seven individuals describe extensive and brazen manipulation of IMPATH's financial accounts.

## Lessons In Lab Management

From this perspective, IMPATH will offer lessons in corporate governance and ethics for laboratory administrators and pathologists. But, at this point, there are no formal charges of specific violations of Medicare and Medicaid laws. Assuming that federal prosecutors take no future action in this area, there are unlikely to be any new legal precedents to affect the Medicare laboratory compliance status quo.

The heart of this crime was the manipulation of IMPATH's financial accounts. In 1999, the company began using a software system called "Impulse." This system tracked testing and billing activity for each specimen and would generate an invoice when testing was completed. But Impulse was not linked to IMPATH's general ledger. The staff manually posted revenue and accounts receivable items to the general ledger.

## Exploiting A System Flaw

The defendants exploited this flaw in the system. Beginning in 1999, "all defendants except McKie routinely inflated Physicians' Services revenue and accounts receivable to match the projections that management handed to the board." The six defendants "simply 'plugged' millions of dollars of fictitious revenue and accounts receivable into the general ledger and fabricated documents to conceal the variance between the amounts in Impulse and the general ledger."

This is the classic "Ponzi Scheme" dilemma. Once the defendants started down this path, not only was it impossible for real-world specimen and revenue growth at IMPATH to grow fast

# Understanding Fraud at IMPATH

**WHEN IMPATH FILED AMENDED TAX RETURNS IN EARLY 2005,** the true magnitude of the fraud engineered by its indicted ex-executives became visible. Revised financial statements, prepared by forensic accounts, show that, instead of the pre-tax profits of $19.5 million and $18.4 million that IMPATH publicly reported in fiscal years 2001 and 2002, respectively, the company actually lost about $11.8 million in 2001 and $14.4 million in 2002.

IMPATH's accounts receivable numbers were the subject of much attention by the investment community during 2001 and 2002. Revised financial statements prepared by forensic accountants indicate that, by 2002, the indicted ex-executives overstated accounts receivable by as much as 61%! The table at right compares the impact of these financial manipulations on IMPATH's publicly-released earnings reports for the four-year period of 1999-2002.

**INFLATING IMPATH'S FINANCIAL REPORTS**

| (In $ millions) | 1999 | 2000 | 2001 | 2002 |
|---|---|---|---|---|
| ***Accounts Receivable, Net*** | | | | |
| Original Form 10-K | $35.5 | $50.7 | $63.6 | $69.0 |
| Adjusted amount | $25.6 | $35.9 | $39.5 | $26.9 |
| Percentage difference | 28% | 29% | 38% | 61% |
| ***Net Revenue*** | | | | |
| Original Form 10-K | $85.4 | $138.2 | $189.6 | $188.1 |
| Adjusted amount | $70.9 | $123.9 | $163.3 | $165.3 |
| Percentage difference | 17% | 10% | 14% | 12% |
| ***Income (Loss) Before Taxes*** | | | | |
| Original Form ˇ | ($0.8) | $8.4 | ($11.8) | ($14.4) |
| Percentage difference | N/A | 63% | N/A | N/A |

*Source: Securities & Exchange Commission*

enough to cover the gap, but the need to fraudulently inflate ever-greater numbers each quarter created exponential growth in the fraudulent totals. Federal prosecutors point this out, stating that "by the fourth quarter of the fiscal year ended December 31, 2002 ("FY2002"), these specially-marked entries to the revenue accounts totaled $24.2 million and accounted for approximately 50% of the revenue recorded in that quarter."

## The Impossible Scam

That means half of IMPATH's recorded quarterly revenue was fraudulent by the end of 2002! That becomes an impossible scam to sustain. The defendants looked for other sources to sustain the fraud. Among other things, they routinely capitalized certain operating expenses and mis-categorized other accounting entries to help manufacture a greater amount of net earnings for the company.

As the table above illustrates, in fiscal year 2002, IMPATH's publicly-declared income before taxes was $18.4 million. Forensic accountants later determined this number was actually a loss of $14.4 million. On adjusted net revenues of $165.3 million, the net income change discovered by forensic accountants totaled $32.8 million, or 20% of revenues.

Saad, Adelson, and Cammarata were also indicted for undisclosed self-dealing. In one instance, they "misappropriated" $851,000 in IMPATH funds to exercise stock options in the first quarter of 2001. In so doing, the defendants used IMPATH's money to fund their stock options, essentially giving them interest-free loans from the company. These actions were neither authorized nor known to the board of directors. Nor did any public filings and proxy statements filed with the SEC disclose these facts.

## Indictment Against Anu:
# It's *Saad*, But True!

THERE ARE INTERESTING BACKSTORIES to the unfolding disclosures in the IMPATH, Inc. criminal investigation. Many center around Anu Saad, Ph.D., ex-IMPATH Chair and CEO.

On April 1, when Federal District Judge Jed Rakoff entered the courtroom for the arraignment of Saad and ex-IMPATH President Richard Adelson, he found Saad was missing.

"You think this is the Michael Jackson trial? Where is she?" queried Rakoff. Saad showed up about five minutes later and heard an earful from an aggravated judge about arriving on time for future court dates.

Photo: Steve Hirsch, NY Post

**A FUTURE JAILBIRD?**
After a late arrival to the courtroom, Anu Saad, Ph.D., former Chair and CEO of IMPATH, Inc., gets dressed down by an irate Judge Jed Rakoff at her first hearing in Manhattan on April 1, 2005.

Although federal authorities stated that Saad was late to court because of her arrest and processing that morning, former employees of IMPATH tell THE DARK REPORT that arriving late to a meeting is a characteristic of Saad. "Anytime someone else called a meeting, it was expected that Anu would arrive late," said one ex-coworker. "She would consistently arrive after the meeting had started. She had a need to always make a grand entrance."

THE DARK REPORT has also learned of another oddity about Saad. After IMPATH's New York and Los Angeles laboratories were remodeled, all doors into the executive suites were locked. Employees could not enter executive suites at either location without a pass code or permission of the receptionist. Further, Saad's office in both facilities included a full bathroom with shower and walk-in closet. This allowed her to further isolate herself from interaction with other IMPATH employees.

As described by federal prosecutors, the defendants engaged in an audacious plan to inflate IMPATH's revenues and net profits for their self-enrichment. It is likely that this is not the only area of ethical lapse by these individuals. For example, when IMPATH agreed to pay $9 million to settle charges of Medicare Fraud and Abuse in October 2001, THE DARK REPORT pointed out that this settlement was both unusual and unsettling.

That's because IMPATH had billed Medicare for control tests for the period 1990 through 1998. Laboratorians understand the implications of this settlement. Among Medicare's "Ten Commandments" for laboratory compliance, "Thou Shalt Not Bill for Controls" ranks high. The fact that IMPATH management was willing to bill Medicare for controls for nine years speaks volumes about its internal controls, compliance reviews, and a cultural ethics that either couldn't identify and fix this non-compliant practice—or looked the other way until the company was caught.

## Compliance Deficiencies?

Viewed in the context of the Medicare fraud and abuse settlement and the current federal charges against its ex-executives, it is not a leap of faith to believe that if more rocks were turned over, additional serious and illegal business practices (particularly in coding, billing, and collections) would likely be found to have occurred during those same years.

THE DARK REPORT believes the current federal charges against Saad, Adelson, and their fellow conspirators are unlikely to have a wide impact on individual laboratories and pathology groups across the nation. That's because these charges relate to financial and securities fraud committed by a group of individuals willing to commit major fraud for financial gain. In so doing, they incurred great risks and are finally reaping the harvest of those illegal and unethical actions. TDR

# Saad & Adelson's Financial Scam Unravels When Bank Audits Collateral

**BY THE END OF 2002,** fraudulent manipulation of IMPATH's financial accounting system was nearing unsustainable levels. Federal prosecutors say that, in its fourth quarter 2002 financial report, such false entries accounted for 50% of the company's stated quarterly revenue of about $50 million.

Soon, three of the key executives of this fraud would no longer be in position to cover their tracks. IMPATH's board ousted CEO Anu Saad in February 2003. Publicly, it stated her resignation was linked to "a lapse of corporate integrity." It was also stated that Saad would repay $250,000 to the company, but no details as to why were provided.

Next out the door was COO Richard Adelson. IMPATH announced his resignation on May 14, 2003. He was followed two days later by CFO David Cammarata, who resigned on May 16, 2003. Even with these individuals gone, the financial accounting manipulations continued. But the clock was finally ticking on this scam.

## How The Scam Unravels

The story which follows is exclusive to THE DARK REPORT. It was pieced together from a number of individuals who once worked at IMPATH. Even after the departure of Saad, Adelson, and Cammarata, other defendants in the financial and accounting department continued to sustain the scam by continuing to make fraudulent entries.

Essential to this scam was the existence of two sets of books, known only to those participating in the financial manipulation. These books showed the real numbers in the Impulse software system which tracked incoming specimens and lab tests, then generated invoices. There was another set of "false" books. These incorporated the fraudulent entries which supported the manual journal entries into IMPATH's general ledger.

It was in late June and early July, 2003 when the scheme to defraud IMPATH and its stockholders was discovered. IMPATH held a credit facility syndicated with **Fleet National Bank** as the leader. This credit facility was secured by IMPATH's accounts receivables and other assets.

According to several knowledgeable sources, in late June and early July, 2003, it was time for Fleet Bank to visit IMPATH's offices and audit the collateral securing this credit line. What happened next is the classic undoing of so many criminal enterprises.

## Unintended Consequences

As Fleet's auditors requested the documents necessary to examine IMPATH"s accounts receivables, an employee unwittingly gave them the "wrong" set of books. Instead of handing the falsified records (which supported the corporate general ledger), the individual instead provided the accurate, real financial records produced from the Impulse system.

It didn't take long for the auditors to see the discrepancy. IMPATH's real accounts receivables were substantially less than believed. Finally alerted to this fraud—and its magnitude—IMPATH's board was forced to issue the fateful press release of July 30, 2003. It stated "the Audit Committee of the Company has initiated an investigation into possible accounting irregularities involving its accounts receivable which the Company believes have been overstated. The Company noted that, given the preliminary stage of the investigation, it cannot determine the financial impact but believes that it will be material."

IMPATH was now launched on its death spiral as an independent company. It was delisted by NASDAQ on August 22, 2003 and would be in bankruptcy court just five weeks later. Following the July 30, 2003 announcement by IMPATH, investors holding its stock lost a cumulative total of one-quarter billion dollars. The magnitude of this loss played a role in the decision by federal prosecutors to prosecute this case.

# LabCorp Buys Esoterix For $150 Million in Cash

*"Low" sales price surprises observers, another competitor removed from market*

***CEO SUMMARY: Laboratory Corporation of America continues to display an appetite to grow by acquisition. However, its purchase of Esoterix, Inc. creates unique management problems for LabCorp, because Esoterix is itself a product of a lab acquisition strategy. Over the past ten years, Esoterix acquired national specialty labs in coagulation, endocrinology, flow cytometry, and allergy testing.***

"CASH IS KING." That is one reason why **Laboratory Corp-oration of America** will soon be the owner of **Esoterix, Inc.**

In a deal announced by both companies on March 30, 2005, LabCorp will pay approximately $150 million in cash to acquire Esoterix, based in Austin, Texas. Observers considered this to be a relatively low price, given Esoterix's annual revenues, estimated to be around $130 million.

The deal was cash and the price was relatively low because LabCorp drove a tough bargain with a seller who needed to consummate a sale to meet a looming deadline. An added factor in the mix was the significant decline in flow cytometry reimbursement which took effect on January 1, 2005. Flow cytometry cases represent a significant portion of Esoterix's case mix.

Cash was the driver in this deal because the seller, **Behrman Capital LLC** of New York City, had a pressing need to liquidate its shares in Esoterix. Back in 1994, Behrman Capital's first investment fund provided the original capital to launch Esoterix. This fund had a ten-year life. In order to close out the fund and return the money to the fund's investors, Behrman Capital needed to sell its shares in Esoterix.

## Buyer Interest In Esoterix

Sources tell THE DARK REPORT that LabCorp showed interest in acquiring Esoterix on more than one occasion in 2004. But for several reasons, no deal resulted. Two things changed between the fall of 2004 and the present.

First, as noted earlier, the lower reimbursement by Medicare for flow cytometry testing took effect on January 1, 2005. This reduced both net revenue and net earnings at Esoterix and caused the company's valuation to decline in proportion to the effects of lower flow cytometry reimbursement.

Second, Behrman Capital's deadline for closing its investments in its first fund and returning money to those investors was approaching. The closer that deadline loomed, the more motivated Behrman Capital was to strike a deal for Esoterix.

Both companies expect the sale will close second quarter, 2005. The immediate effect of the acquisition will be to remove another competitor from the national marketplace for reference and esoteric testing. The Esoterix deal follows on the heels of LabCorp's earlier purchase of **US LABS, Inc.**, announced last December and closed in March, 2005. *(See TDR, January 3, 2005.)*

## Management Challenges

LabCorp takes on some interesting management problems with its acquisition of Esoterix. Over the years, Esoterix had acquired a number of national specialty testing lab companies. *(See TDR, September 16, 2002.)*

Included in this mix were labs that performed testing in flow cytometry, endocrinology, allergy, coagulation, and a clinical trials division. For LabCorp, integrating these businesses into its existing network of laboratories will prove uniquely challenging.

Following LabCorp's purchase of of **Dynacare**, **DIANON Systems** and **US Labs**, it continued to operate these business units under their original name. Integration and consolidation of these businesses into LabCorp's national testing infrastructure has been low-key and ongoing.

## Integration Issues

Based on this pattern, it is likely that LabCorp will continue to use the Esoterix name after the acquisition. At this time, LabCorp has released no details about how it will integrate and consolidate the Esoterix testing resources into its existing system.

Because Esoterix serves a unique blend of customers, including hospitals, office-based specialist physicians, and clinical trials vendors, the acquisition of Esoterix by LabCorp is not likely to disrupt the competitive status quo in the lab services marketplace. TDR

## Ventured-Funded Lab Usually Come to Market

LABORATORY COMPANIES FUNDED with money from venture capital and private equity firms will eventually need to cash out those investors.

Typically, venture capitalists want to harvest their profits about five years after their investment. Private equity funds often have longer horizons, but also need to eventually sell their equity, realize the profits, and pay off their own investors.

These types of investors typically have two options to liquidate ownership shares in their portfolio companies. First, the portfolio company can use an IPO (initial public offering) to sell shares to the public. Second is to sell the portfolio company to someone else. This is the option Behrman Capital is using to liquidate its ownership in Esoterix so it can close out its first investment fund.

In today's market, whenever a venture-backed laboratory company is offered for sale, the most likely buyers are LabCorp and **Quest Diagnostics Incorporated**. Moreover, they are likely to be high bidders over other interested parties. That's because, compared to other classes of buyers, the client list, trained lab staff, and service infrastructure of the selling laboratory often have higher value to either or both of the two blood brothers.

By understanding the business model of the venture capital-funded laboratory company, one can anticipate which laboratory companies will eventually come to market and be offered for sale. Obvious examples that fit this description are **AmeriPath, Inc.** (Palm Beach Gardens, Florida–acquired by **Welsh Carson Anderson & Stowe** in 2003) and **Pathology Partners, Inc.** (Dallas, Texas–funded by several venture capital companies in 1998). Also funded by professional investors are **CBL Path, Inc.** (Ocala, Florida) and **Clinical Pathology Laboratories, Inc.** (Austin, Texas).

# NEWSMAKER INTERVIEW

# Victim of First HIPAA-Convicted Crime Tells Story & Offers Advice to Labs

"I figured the hospital would be subject to a multi-million dollar HIPAA lawsuit if my hospital records were proven breached—which is exactly what happened."
**—Eric Drew, cancer patient and patient identity theft victim**

CEO SUMMARY: Eric Drew's story may be one of the most amazing to have happened in the modern age of laboratory medicine. It is actually two stories, intertwined. In the first, a patient with the nearly-always fatal diagnosis of acute lymphoblastic lymphoma fights for his life, desperately trying one experimental procedure after another. In the second, an employee of the laboratory in the hospital providing these treatments decides this patient, expected to die sooner rather than later, is the perfect victim for identity theft. What the phlebotomist did not count on was that his crime would actually motivate the victim to fight—both for his life and to see the thief of his identity brought to justice. THE DARK REPORT is presenting this exclusive interview with the victim, Eric Drew, as a way to help laboratories and pathology group practices understand how to improve their defenses against patient identity theft committed by their own employees. Pamela Scherer McLeod conducted this interview.

**EDITOR:** In a few short months in 2003 you took on two major battles. The first was a battle for your life after you were diagnosed with acute lymphoblastic leukemia (ALL). The second battle was to stop the financial devastation that was being perpetrated by a laboratory worker at **Seattle Cancer Care Alliance** (SCCA), where you were being treated.

You have survived five leukemia treatment cycles, including three transplant preps and two completed transplants. You single-handedly solved the crime that became the nation's first criminal conviction under HIPAA (Health Insurance Portability and Accountability Act), with the result that identity thief and phlebotomist Richard W. Gibson now sits in a federal penitentiary serving a 16-month sentence, with $15,000 restitution yet to be paid.

Hospitals and laboratories throughout the country will benefit from your first-hand account of how this crime by a laboratory technician happened and your advice on what hospitals and laboratories need to do to further protect their patients against the crime of identity theft. Share with us, please, how this incredible story began.

**DREW:** In December 2002, after feeling ill since about November, I was diagnosed with acute lymphoblastic leukemia (ALL) and told that I had five days to live unless I got treatment. This diagnosis was unexpected. I had just donated platelets for children with leukemia in my home town of Los Gatos, California. I've been an apheresis donor for about ten years. Apheresis is something that my mom had been doing for years. I was immediately sent to **Stanford University Medical Center** for chemotherapy and radiation treatment. That went on for ten months, until September 2003.

**EDITOR:** It was during this time that you started the Drew Foundation to raise money and awareness for leukemia?

**DREW:** Yes, I started the foundation and organized a bone-marrow registration drive in 2003. Nearly 1,000 people showed up. The foundation (*www.drew-foundation.org*) has raised over $250,000 for charities and individual patients. The hours that I spent trying to deal with this identity theft situation were hours that I otherwise would have spent raising money for the foundation.

**EDITOR:** How did you end up in Seattle, Washington at the **Seattle Cancer Care Alliance** (SCCA)?

**DREW:** The chemo treatments at Stanford did not work. My half-sister, whom I had just met a couple of years prior to all this, was working as a physician's assistant in the bone marrow transplant program at the **Fred Hutchinson Cancer Research Center** in Seattle. She immediately flew down to Los Gatos to consult with me about their protocols. On September 9, 2003, I entered the **Fred Hutchinson Cancer Research Center**, which is part of the **University of Washington Medical Center**. SCCA is on the Hutch campus. It is an outpatient hospital where the treatments actually take place. I began undergoing tests on Sept. 10, 2003.

**EDITOR:** How soon afterwards did you become aware that someone had stolen your identity and was on a spending spree using your name and credit?

**DREW:** Only seven to ten days after arriving at SCCA! I began receiving notices from banks and creditors thanking me for credit applications that I had never submitted. This was troubling because, before I started my treatment, I had deliberately closed all but one or two of my accounts at home. I had not opened any new ones. I had not done any business of any kind in Seattle—other than my business with SCCA. There was no opportunity for anyone to access my information, except through the hospital records. It was obvious to me that somebody from the clinic had taken my information. At the time, I realized that the identity thief had figured "This guy has a terminal disease. There's no treatment that can cure him. I can steal his identity and, because he is soon to die, no one will ever try and solve this case."

**EDITOR:** At what point did you notify the hospital or the authorities that you suspected identity theft?

**DREW:** Pretty much right away—as soon as I started getting "thank you for your credit application" letters from credit card companies. I called the Seattle Police Department. They didn't even assign me a case number, much less assign an investigator. They told me they get 100 of these cases a week. I finally became so frustrated with the Seattle police that, in mid-December 2003, I contacted the chief of police in my home town of Los Gatos, California. He's a friend of mine. He did assign me a case number and an officer. But nothing really came of that.

**EDITOR:** What about the people at the hospital? Did you get any help there?

**DREW:** I contacted the compliance office at the University of Washington Medical Center. They were no help at all. They asked me how I knew it was a hospital employee and said that, even if it were, there would be no way to prove it.

In December 2003, I began receiving telephone calls from credit card companies for non-payment. Gibson had opened the first fraudulent credit card in my name, an **AT&T** Universal Card, on Oct. 17, 2003. He ran up $7,180.81 in charges. He bought everything from jewelry and video games to gas, incidental groceries and home improvement merchandise. He was using it for everything.

Eric Drew

"I contacted the compliance office at the University of Washington Medical Center. They were no help at all. They asked me how I knew it was a hospital employee and said, even if it were, there would be no way to prove it."

I had been through unmitigated hell since arriving in Seattle in preparation for a haploid transplant. The procedures were torturous. I went through very painful radiation treatments, spinal injections, chemo poisoning, and bone marrow biopsies. A couple of weeks after I began receiving letters about these new fraudulent applications, I also had gotten disappointing news. The haploid transplant did not offer the 50% chance of survival as I had previously thought. Actually, the chances were only 10% to 15% and I think the doctors were being kind by giving me these figures. I was trying desperately to research and explore alternative solutions to try and save my life. It was a very difficult time for me.

**EDITOR:** You had gotten no help from the police or the hospital. Where did you next turn?

**DREW:** When the "thank you" letters began arriving in September, I started a file. I was trying to piece things together. About mid-December, I

started meeting with Richard Meeks, the HIPAA compliance officer at University of Washington Medical Center. I demanded to know who had access to my records. I wanted to know also how my information had been sent from Stanford to SCCA. I did not get any kind of helpful response. He just said that he was sorry this was happening to me.

I also contacted Aleana Waite, Director of Quality and Patient and Family Services at SCCA. She was like everyone I spoke to in the hospital at this time about the obvious theft of my identity. They were all just telling me there was nothing they could do.

They rolled their eyes and treated me as though I were just some unruly patient. They were very patronizing. I thought later, why would the hospital help me? I figured the hospital would be subject to a multi-million dollar HIPAA violation if my hospital records were to be proven breached—which is exactly what happened!

**EDITOR:** And you were doing this concurrently with your treatment?

**DREW:** I was doing as much as my physical condition would allow to deal with the identity theft and to get it stopped. I was earnestly trying to get someone interested enough to help me. My doctors and my family were all trying to get me to drop it. They kept saying, "Just cancel the accounts, file a complaint, and move on or you're going to stress yourself to death."

That would have all been well and good, but more and more calls from the banks and creditors demanding money kept coming each day. In retrospect, I have to thank Mr. Gibson. He probably saved my life. I was so angry and frustrated and felt so little control in my life on all fronts. I viewed solving my identity theft case as the one thing in my life over which I could take control. I knew something could be done. It's just that nobody, anywhere in the system, was willing to do it. For my part, I believed I knew how to get the information needed to nail this guy.

On December 23, 2003, I had my first bone marrow transplant—a haploid (half-match) with my half-sister Alexa as a donor. She's the PA who had worked in the bone marrow transplant at Hutch for five years. I became very ill after the transplant and was near death several times.

By mid-January 2004, I was feeling exceptionally well, better than expected. On the downside, I had a ton of mail and voice messages from credit card companies, dunning me for late payments. Of course, I had been in no condition to attend to my mail.

I realized that all the police reports and the reports I had made to creditors back in October had gone unheard. That's when I decided, "okay, I'm going to catch this guy." I began spending 10 to 12 hours per day investigating this case. There were even times when I went down to the Seattle docks, scarcely able to walk and tubes hanging from my chest, to talk with some pretty scary characters trying to track down leads. The police, the hospital, the press, nobody was helping me at this time, even though I provided them with a lot of information on what I had found. I had gathered enough evidence to turn the case over to the police on a silver platter. And still they had done nothing.

**EDITOR:** How did you go about it? What steps did you take?

**DREW:** I had once been Vice President of a mortage banking firm. I was very familiar with the credit reporting industry. I knew that it was one source of information that could help solve this crime. However, when I directly contacted the three national credit repositories, as a consumer, to notify them of the identity theft and ask for detailed information about transactions occur-

ring under my name, they were not cooperative.

So I did something that is unavailable to most consumers. With the help of some friends in the mortgage banking business, we ran the type of detailed credit profile that is available to lenders. By combining that information with the credit card statements I was receiving, I was able to learn to which address the new credit cards were being delivered. I then contacted a real estate title company and obtained the name of the owner of the residence at that address.

I sent a letter to the owner of the residence and later received a call from a woman who said she was the owner's mother. The owner, it seems, was in the pen serving 30 years for murder. She gave me the name of Keisha Gibson, who was living at the residence with her two children, ages eight and five. I telephoned Keisha Gibson, who was working as a legal secretary at the time. I told her why I was calling. She said she did not know what was going on—that someone else might be using her mailbox.

Eric Drew

"You can't imagine how frustrated I was that no one would make the slightest effort to help—police, banks granting credit under my name, credit agencies, and now the hospital."

When I realized I had the likely address for the identity thief, I contacted the post office that served that area and obtained the name of the manager and the route carrier. I asked them why they were delivering mail with so many different names to one address where only a woman and two children lived. They simply answered that the **United States Postal Service** was unable to manage situations like that. It just delivers mail as addressed.

About this time I actually went out and took photographs of the house, which had a fancy new barbeque grill out front. I didn't know it at the time, but that grill had been bought with one of the credit cards opened under my name!

**EDITOR:** Did you notify the police?

**DREW:** Absolutely! I turned this information over to the Seattle police, to a Detective Al Thompson. I called Richard Meeks again, the compliance officer at the University of Washington Medical Center (UWMC). And I also called Aleana Waite at SCCA. I gave them the name Keisha Gibson and the address I had found to which the cards were going. I requested that they check their employee records to see if there was, or had been, anyone named Gibson in their employ during the time I was a patient. I was very disappointed at their response. They told me they ran a check to see if any employee lived at the Keisha Gibson address. But but they did not offer to check their employees for a "Gibson." Nor did they share with me any knowledge that someone named "Gibson" might have been working anywhere near the areas where I had been a patient, at the time I was in their hospital.

**EDITOR:** It strikes me that this was an opportunity for the hospital to "do the right thing" and investigate the possibility that a "Gibson" working for them might have been in a position to have accessed your confidential data.

**DREW:** That was both my expectation and hope. You can't imagine how frustrated I was that no one would make the slightest effort to help—police, banks granting credit under my name, credit agencies, and now the hospital.

**EDITOR:** Did the information you provided to the hospital make a difference?

**DREW:** Nothing that proved helpful or stopped Gibson's continuing to open fraudulent accounts in my name. These hospital officials just kept telling me

they checked their records and nothing showed unauthorized access to my information.

**EDITOR:** THE DARK REPORT understands that you issued a press release about your identity theft case.

**DREW:** Yes. I had drafted a press release describing the details of my circumstances and what was happening to me—that while I was seeking treatment for a usually-fatal form of cancer at SCCA, a healthcare worker right there in Seattle had stolen my protected information. This thief was running up thousands of dollars in charges. He was getting away with it and the authorities were being of no help whatsoever. I disseminated the press release to every media outlet I could think of: the Seattle Police Department, the Seattle Mayor's Office, the FBI, the City Attorney, the Washington state Attorney General's office, the U.S. Attorney General's office, the U.S. Attorney's office in Seattle, CNN, NBC, local newspapers, and local radio and television outlets.

**EDITOR:** Surely you got someone to respond?

**DREW:** After the press release, the Seattle mayor contacted the head of fraud at the police department, a Detective Eng. Eng then instructed Detective Thompson to take a statement from me. They finally took a statement and gave me a case number. That was it. It never went anywhere from there. I never got any kind of help from them.

**EDITOR:** What happened when you contacted the FBI?

**DREW:** The duty officer gave me the impression that the FBI did not care. He said to call the Secret Service, that they were now the agency which handled fraud. He said to call back later and hung up on me. He was rude. I called the FBI so many times, they threatened to put a restraining order on me.

**EDITOR:** What about the banks in all this? Were they any help?

**DREW:** Hardly. It's a situation where the right hand of the bank has no idea what the left hand is doing. I felt more violated by the banks than by Richard Gibson. I consider them to be the biggest enablers in all this. Their policies and procedures are what make identity theft ridiculously easy for the bad guys.

Eric Drew

"I felt more violated by the banks than by Richard Gibson. I consider them to be the biggest enablers in all this. Their policies and procedures are what make identity theft ridiculously easy for the bad guys."

For example, on November 11, 2003, **Chase Bank** sent me a letter about being delighted that I had applied for an account with them. The letter also stated that, if I, in fact, had not applied for the card, I should call them right away. If they did not hear from me, they would continue to process the application. Of course, Chase Bank had no procedure to cover a situation where someone was too ill—or out of pocket for any reason—and thus not available to respond. It's a stacked deck—and not in favor of the consumer!

Here these banks take information from anybody, and, with no verification, open these credit card accounts. Then, later, when I notify them of the fraud, they wanted me to provide them with all kinds of affidavits and other proof of identity to close the fraudulent accounts! It was the same with the credit reporting agencies. **Equifax** informed me that I would have to submit a signed affidavit and proof of identity documents. All the burden is put on the honest consumer. And these things take an incredible amount of time; it's very disruptive to someone's life. The banks know that they are still coming out ahead. They're still making money. This is just the cost of doing

business for them. But it's a nightmare for consumers who find themselves victims of identity theft.

**Capital One** did send me a letter of inquiry because the addresses did not match up. **CitiCorp** sent me an identity theft tool kit. I also learned that Gibson had made a $5,700 payment to them on a Nevada bank.

**EDITOR:** Your perseverance was remarkable, to say the least. What finally happened that led to Gibson's arrest?

**DREW:** My big break came when **KING5 Television**, the local NBC affiliate, called and wanted to interview me. They had received the press release. The hospital didn't want me to do the interview. I was in the middle of a treatment and had tubes all over. I was having three transfusions a day, just to stay alive. I demanded that they stop the treatment and told them I would pull out all the tubes myself if I had to, but that I was going to do that interview.

**EDITOR:** On February 11, 2004, KING5 news aired a segment. I'd like to share part of the broadcast: "Cancer patient is victim of ID fraud... Eric Drew, 36, a leukemia patient fighting for his life, said someone has stolen his identity and made thousands of dollars in purchases."

**DREW:** The TV interview raised everything to a whole new level. KING5 aired it several times a day. Suddenly, everybody got interested.

**EDITOR:** Who contacted you at that point?

**DREW:** After my story aired on the TV news, I was contacted by Aleana Waite and Julie Hamilton, the privacy officer at SCCA. They said they were very sorry this had happened to me and asked if there were any way they could help.

**EDITOR:** Was this the first time the hospital proactively offered support?

**DREW:** Yes, but it was an offer, not action. Remember, they had the name "Gibson" and had still not offered me any specific information about whether or not someone with that name might have been employed by them and had access to my patient records.

**EDITOR:** How did you push your investigation, now that the TV news broadcasts were bringing attention to your plight?

**DREW:** Weeks earlier, I had contacted retail stores where Gibson had used the fraudulent credit cards. I had asked them to check their surveillance tapes. At that time, no one would help. That changed once the TV news feature was broadcast. A public communications officer at **Lowe's Home Improvement Centers** called and offered to help me. Lowe's gave me the date and time of the purchase where Gibson had bought some home improvement materials. They could not turn the surveillance tape over to me; they said they could only turn it over to the police. Chris Daniels, the KING5 reporter who had interviewed me, called Detective Thompson at the Seattle Police Department. He told the detective that if he would get the tape, KING5 would air it.

On Thursday, February 26, 2004, KING5 aired the surveillance tape showing Gibson making the purchases at Lowe's. That blew the lid off! People started calling the police station, the TV station, the hospital. They identified the thief as Richard Gibson, 42, a laboratory employee of SCCA. Chris Daniels, the KING5 reporter who was helping me, called me to tell me the news. They had a positive identification of the perp. It was a vindicating moment!

**EDITOR:** You must have been excited about this break in your case.

**DREW:** Yes. The next morning, on Friday, I had to go back to SCCA's lab for more transfusions. Gibson had not shown up to work. The people in the lab were very upset. Some were crying. They couldn't believe it had been someone in their lab. The phlebotomist that drew my blood avoided looking

# Up Close & Personal: Watching Gibson

**WHEN PATIENT ERIC DREW LEARNED** who had stolen his identity and was charging thousands of dollars to credit cards opened in his name, it was someone he saw daily while a patient in the hospital.

**EDITOR:** What type of interaction did you have with Richard Gibson when you were being treated at Seattle Cancer Care Alliance (SCCA) in Seattle?

**DREW:** I saw Gibson virtually every day that I was in the lab. He had worked there for three years. The phlebotomy area at SCCA has about ten tables where they draw blood. There was a counter and window pass-through with the laboratory area on the other side. That's where Gibson worked. I saw him every day working in that lab area.

**Now A Jailbird:** Left photo is convicted phlebotomist Richard Gipson at his arrest. Right photo is Gipson arriving in court. His HIPAA conviction put him in a federal penitentiary for 16 months.

**EDITOR:** Was this at the time he was stealing your identity?

**DREW:** Yes. For example, on November 11, 2003, he used my information to open the Chase account. On November 28, 2003, he opened the **Bank One First USA** Visa. He ran up $1,958.61 on that. All this time, he was seeing me, a desperately-ill patient in that next room, each day through that window. Of course, these details unfolded after I launched my own intensive investigation.

**EDITOR:** So he knew your disease was likely to prove fatal?

**DREW:** Without question. At this point, it had been one setback after another in my desperate efforts to find a treatment that would save my life. At this point, most people who underwent a haploid transplant had died. How could this guy have been back there, seeing me almost everyday, knowing what I was going through? From the time sequence we reconstructed, he had to have ripped off my information within days of my first admission to SCCA for treatment. He knew exactly what he was doing.

**EDITOR:** What do you mean by that?

**DREW:** It was how Gibson went about his theft of my identity. For example, he used the ATM machine at the medical office building next to the **Swedish Medical Center** (SMC) near where I was living. He used to work for the laboratory there. He knew there was no surveillance camera in the lobby where the ATM was located. He even activated one of the credit cards from a Dr. Robert Kitchell's office, an internist in that medical building. When I found this out, I called Dr. Kitchell's office and was told the number used was an employee telephone and they had no one there by the name of Gibson.

**EDITOR:** Since he was a phlebotomist and had formerly worked in the laboratory at SMC, it's likely he knew the staff at Dr. Kitchell's office, knew about the employee phone there, and knew no one would challenge him coming in and using that phone—a number difficult to trace back to him.

**DREW:** That would explain why he used the phone in Dr. Kitchell's office. In fact, there was a gift shop in the lobby of Swedish Hospital, Margo's Card Shop. This showed up on the credit card statements. Gibson rang up almost $300 there buying Christmas gifts. The manager remembered him because it's a card shop and the guy bought so much merchandise. When the TV reporter talked to him, he remembered Gibson well and gave a complete description of him. The guy said he had even helped Gibson carry the purchases out to his car.

me in the eye. KING5 interviewed me again that day, along with Norman Hubbard, the COO at SCCA.

**EDITOR:** What about law enforcement? What did they do, now that you single-handedly solved the crime for them—that is, you and the TV reporter?

**DREW:** On March 2, 2004, four days after the TV broadcast of his photo and almost six months after this nightmare started, Richard Gibson turned himself in. KING5 got footage of him walking into the police station with his attorney. Chris Daniels, the KING5 reporter, shouted with a microphone pointed toward Gibson, "What do you have to say to Eric Drew?" Gibson's attorney just said, "No comment."

**EDITOR:** So how did the case proceed?

**DREW:** It was appalling. The prosecutors in Seattle did not know how to press charges against him, even though I had all the evidence against him in the file I had spent months building. So, after 24 hours, they released him against a small amount of bail. This, even though they had the surveillance video tape of him engaged in criminal behavior.


"It was appalling. The prosecutors in Seattle did not know how to press charges against him, even though I had all the evidence on him in the file I had spent months building. So they let him go. "

**EDITOR:** That's amazing! What did you next do?

**DREW:** This turn of events surprisingly worked in my favor. Within a day of Gibson turning himself in, I again contacted the U.S. Attorney's office in Washington, DC. I was determined that Gibson be prosecuted as a HIPAA violation. I was told they had heard of my story and they finally agreed to assign me some help. The national office referred me to the head federal prosecutor in Seattle, Vince Lombardi—I believe he's the grandson of Green Bay Packer Head Coach Vince Lombardi. Lombardi called me a couple of days after the arrest and told me that he was assigning a U.S. attorney and an FBI special agent to my case.

**EDITOR:** Was this a serious investigation?

**DREW:** Assistant U.S. Attorney Susan Loitz was assigned to prosecute the case. FBI Special Agent James Rogers spent about six months investigating it. Using the file I had amassed, he pulled the pieces together. By now, I knew this would be federal prosecution against someone for a criminal violation of the new HIPAA laws which were intended to protect patients.

**EDITOR:** HIPAA does provide for sanctions against providers which disclose confidential patient information. How did that play a role in the decision to include or exclude SCCA from any legal action?

**DREW:** The U.S. Assistant Attorney had a number of statutes under which they could have proceeded. I told Susan Loitz that I didn't want them to go after the hospital. They are good people. They just screwed up by not listening to me.

**EDITOR:** That's a charitable view, considering your earlier statements about their unwillingness to say much more than that "we have no evidence of unauthorized access to your patient information."

**DREW:** True, but the bad guy in this episode is Gibson and I wanted him to face the consequences of his crime.

**EDITOR:** What is going on with phlebotomist Gibson during this time?

**DREW:** Gibson was out walking the street. He must have thought he was going to get off scott-free.

**EDITOR:** Didn't Seattle Cancer Care Hospital, now that they had Gibson's identity, fire him?

**DREW:** Yes, but he was certainly unconcerned about his crime and its potential

consequences. After SCCA fired him, he continued to work at **Seattle Community College**, where he was teaching phlebotomy at one of the local community colleges. He also had the temerity to not only apply for unemployment benefits, but he then filed an appeal when his claim was denied. He admitted to everything in his claim. The Administrative Law Judge's Order lays out how Gibson admitted to taking my private patient information while he was employed at SCCA and using it for personal gain—with the knowledge he was violating the law. Also, Gibson had claimed that he did not know that I was a patient at the time he fraudulently used my information.

**EDITOR:** Did he ever say how he got your information while you were in the hospital?

**DREW:** Well, the only statement he made to the authorities was a story he told the Administrative Law Judge at the unemployment appeal hearing. He stated that he had found my information on a piece of paper lying on the floor of a men's bathroom inside the hospital.

**EDITOR:** What did SCCA tell you about how they thought he got access to your private information?

**DREW:** SCCA's response was a non-response. All they would say is "we've checked our systems and we have no evidence that any unauthorized individual accessed your records."

**EDITOR:** So what is the next development in the case?

**DREW:** In June 2004, the U.S. Attorney's Office came to me and said that they wanted to offer Gibson a low sentence in response to his agreement to plead guilty. They asked if I would agree to it. I told them I did not care what specific penalty he received for his crime, so long as they charged him under the federal HIPAA statute. That's because I had no confidence in the Seattle Police Department. I wanted the federal court to take responsibility. After what I had been through, I wanted to establish some legal precedent so that no one else would have to go through what I went through. The FBI put me in the federal witness protection and assistance program. I began working with the hospital to help them clean up the mess created by this identity theft case.

**EDITOR:** What happens next in your story?

**DREW:** By the last part of June, 2004, I had again traveled from California to Seattle for a second half-match bone marrow transplant. When I checked back in at the lobby of SCCA, the admitting receptionist was going over all of my information with me again. Here was all my critical demographic-identifying information—right there in the lobby of a busy hospital! My social security number, financial data, and personal information were all on that piece of paper, visible to anyone that might handle my file. After everything I had gone through, I was most unhappy about this situation!

Eric Drew

**"I can certainly imagine how that paper file, as it traveled around Seattle Cancer Care Alliance, could have been viewed by any employee. Moreover, how would the hospital have any way to know who saw my paper patient records?"**

**EDITOR:** Is that because you now appreciate the risk that paper records generate in a hospital or physicians office?

**DREW:** That's a hot button with me. I complained about that situation to the receptionist. And I can certainly imagine how that paper file, as it traveled around the Seattle Cancer Care Center and back to the records storage, could have been viewed by any employee. Moreover, how would the hospital have any way to know who saw my paper patient records?

**EDITOR:** Controlling access to paper files is something that should now make every hospital, laboratory, and pathology group practice nervous about their vulnerability to an employee intent on committing a patient identity theft crime. What happens to you next?

**DREW:** Everything was ready to go on the second transplant when it was decided that I needed to go through a much more aggressive and dangerous experimental procedure—one that was not available at SCCA. So I traveled to the **University of Minnesota in Minneapolis**. Here I underwent a very experimental cord blood transplant, using cords flown over from Italy. This seemed to be my best chance for long-term survival. While I was in Minneapolis, two FBI agents came to the hospital. From my hospital bed, they video-taped a three-minute victim impact statement from me. This was played at Gibson's sentencing.

**EDITOR:** What was Gibson's sentence?

**DREW:** He is currently serving 16 months in a federal penitentiary. He must also pay restitution of about $15,000. He was sentenced on November 5, 2004, about 14 months after he launched his crime against me.

**EDITOR:** Eric, yours is an astonishing story. In concluding this interview, you have an opportunity to address the major players in laboratory medicine in this country. What recommendations would you offer them about how they can improve protections against patient identity theft in their laboratories?

**DREW:** First, laboratories should severely limit which employees have access to a patient's sensitive demographic information. Sensitive information needs to be kept in secure electronic files with secured access only to those authorized to see such information.

**EDITOR:** You are emphasizing an electronic records system. What about paper records?

**DREW:** Any hard copies that are kept should be stored in a locked vault with restricted access. As a patient, I would prefer to know that anyone having access to any of my confidential information should be required to have some sort of official clearance or licensing, just like a notary public, for example. Medical facilities should be required to use something other than social security numbers on their records. Anyone working in a medical lab should have to go through some type of intense screening as part of the hiring process.

**EDITOR:** How should a laboratory or pathology group practice respond when a patient notifies them of a possible breach in their personal and confidential information?

**DREW:** When a patient alerts a facility that they suspect identity theft has occurred, by all means that facility should take that patient seriously. Employees must listen closely to the patient. The healthcare facility should have an established protocol for investigating their employees who have had access to protected information. I want to emphasize that this is an easy crime to commit. Laboratories must become alert to this threat.

**EDITOR:** Thank you, Eric, for your time in sharing this remarkable story with us. You have our sincere wishes for a long and healthy life.

**DREW:** I'd like to thank you for the opportunity to speak out. As your readers have learned, my biggest frustration was that, as a single and very sick patient, no one and no part of the system would listen to me and help me until the television news got involved. Please remember that fact. Whenever a patient surfaces with a suspicion or episode like mine about identity theft, I'd like to think that laboratory folks will remember this story and respond effectively to this patient. TDR

*Contact Eric Drew at 408-354-9640*

# Avoid Patient ID Theft With Proactive Steps

*Eric Drew's remarkable story reveals vulnerability of every lab to this crime*

***CEO SUMMARY:*** ***Identity theft is one of America's fastest-growing crimes. Not only that, it is simple to commit and can be done by anyone. Few laboratories and pathology group practices are prepared to deal with the crime of patient identity theft. Labs should proactively move to implement protections against patient identity theft and raise the awareness of employees to this type of crime.***

**By Robert L. Michel**

PATIENT IDENTITY THEFT WILL SOON be on the radar screen of all healthcare providers, including laboratories and pathology group practices.

As a criminal trend, it is still in its infancy, but it has the potential to grow on a scale unforeseen by experts. Further, under HIPAA (Health Insurance Portability and Accountability Act), patient identity theft represents an entirely new dimension of risk.

THE DARK REPORT recommends that all laboratories and pathology groups should take steps to understand this crime and implement safeguards against it. To help in that effort, we are proud to bring you the exclusive interview with cancer patient Eric Drew.

His story is remarkable, amazing, and inspiring, for many reasons. But it is also troubling. I suggest you carefully read the full interview on pages 9-19. It is complete and detailed for a reason. In his own words, Eric Drew shows you how easy it is for someone inside a hospital laboratory to steal a patient's identity and profit from the crime. He also shows you what happens when the healthcare provider is unprepared to deal with a patient who is a victim of identity theft while under its care.

I call your attention to several points, assuming that you have read Drew's interview before you read my commentary. First, Drew acted within the system. Realizing his identity was stolen and wiht good reason to suspect the crime occurred in the hospital where he was a patient, he used the "privacy hotline" at

the hospital to notify them of the situation. Hospital officials met with Drew.

What was the hospital's response? In Drew's words, "They rolled their eyes and treated me as though I were just some unruly patient. They were very patronizing. I thought later, why would the hospital help me? I figured the hospital would be subject to a multi-million dollar HIPAA violation if my hospital records were to be proven breached—which is exactly what happened!"

Put your lab or pathology group in the same scenario. Who would meet with a patient that had a sound argument, based on early evidence, that someone within your organization had committed the crime of patient identity theft? What would be their response, in speaking for your laboratory?

Here is where the ethics of your laboratory will become visible. Eric Drew's hospital took what was, essentially, a position which was both do-nothing and adversarial. Drew said "They asked me how I knew it was a hospital employee and said that, even if it were, there would be no way to prove it."

This rubs against my business ethics. If I had evidence that an employee was engaging in criminal behavior at work, I would certainly want to jump on this case, learn the facts, and, if warranted, terminate this individual at the earliest opportunity. In Eric Drew's case, once briefed about the identity theft, this healthcare provider showed no motivation to either help him in tangible ways, nor did it immediately initiate internal actions to identify the culprit and take effective action against that employee.

I should point out that the hospital's attitude toward this case of patient identity theft was not much different than that of the Seattle Police and the FBI. What made the difference in Eric Drew's case was that he got media attention. Once television news broadcasts publicized the fact that a patient battling an almost-always fatal form of cancer at **Seattle Cancer Care Alliance** (SCCA) was also battling patient identity theft—from his hospital bed—he did get a higher degree of attention from his healthcare provider and the authorities.

But even that attention did not translate into an effective response to his situation. I wonder what might have happened had the CEO of SCCA, or the CEO of **University of Washington Medical Center,** publicly leaned on the Seattle Police and District Attorney to pursue and prosecute Drew's case. This did not happen, but I ask the question. Would your laboratory be prepared to publicly support justice for a patient who experienced identity theft while under the care of your laboratory? Keep in mind, some would view that as negative publicity even though it would be the right thing to do.

## Tough Actions—What If?

In fact, let me ask this. If Eric Drew's hospital had taken the tough stand on this crime; if it had worked to ferret out the criminal among its employees; if it had put pressure on the police and district attorney to successfully prosecute the case: wouldn't that have been the win-win decision for everyone?

Patient Eric Drew would have not only seen justice done, but would have been grateful to the hospital. The hospital would have sent a powerful message to the community—and its employees—that it is tough on crime and not to be messed with.

My final point is probably the most obvious. If patient Eric Drew had chosen to find a high-profile attorney, the evidence indicates that he would have a strong civil case against the hospital. He has already made that connection, as noted in the quote earlier. In fact, it appears the hospital's reaction was organized more to neutralize the threat that this patient might have standing to sue than to deal effectively with the crime and bring it to a resolution that satisfied all parties. TDR

# INTELLIGENCE LATE & LATENT

*Items too late to print, too early to report*

This may be one of the laboratory industry's biggest "oops" ever! As part of a laboratory proficiency testing program, 4,000 laboratories in 18 countries were sent live samples of the H2N2 flu virus. In 1957, H2N2 is believed to have caused between one and four million deaths. Last week, the **Centers for Disease Prevention and Control** (CDC) went public with its concerns and an order for all laboratories to destroy the live virus. This episode demonstrates how changing healthcare standards can affect overlooked sectors of healthcare services.

### *MORE ON: Proficiency Test*

For the **College of American Pathologists**, (CAP), this is proving to be a significant public relations gaffe. **Meridian Bioscience, Inc.**, of Cincinnati, Ohio, had been shipping proficiency testing kits with the live H2N2 flu virus since last September to labs participating in the proficiency programs of CAP, **Medical Lab Evaluators**, the **American Association of Bioanalysts** (AABA), and the **American Association of Family Practitioners** (AAFP).

## FLORIDA DOCTORS ESTABLISH THEIR OWN MEDICARE HMO

In Miami and Dade County, Florida, 175 physicians provided the venture capital funding to launch **DoctorCare**. It is a doctor-owned and doctor-managed private Medicare insurance company. DoctorCare opened for business in January, following a two-year effort to obtain state and federal licenses. It has a simple concept. Eliminate administrative hurdles and barriers and allow physicians to provide the care they believe is needed by their patients. DoctorCare is starting with 650 physicians and 500 patients. It expects to add about 5,000 new Medicare beneficiaries annually. DoctorCare was also recently selected by **UnitedHealthcare** as a provider for the insurer's 10,000 Medicare beneficiaries in the Miami-Dade County area.

### *ADD TO: DoctorCare*

DoctorCare is an example of how the free market can work. Its physician-owners believe they can operate an insurance plan more effectively than the health insurance industry. Joseph Caruncho is CEO of **PreferredCare**, the only other provider-owned Medicare insurance plan in the Miami area. He said, "I see this model taking root in the future. Doctors don't need training wheels anymore. Doctors are fed up with HMOs. They don't have a lot of impact other than diverting a lot of funds [to administrative costs]." DoctorCare will provide an interesting case study. Its physicians will be under the same pressure to manage utilization against a fixed premium as other insurers.

---

### *WHERE ARE THEY NOW?*

IMPATH, Inc.'s turbulent years of 2002 and 2003 caused a number of its higher-level staff to resign and find positions in other laboratory companies. Here's where some ended up. • Heather Creran, formerly IMPATH's V.P. of Operations, is now at **Clarient, Inc.** (formerly known as **ChromaVision Medical Systems, Inc.**). • Marilyn Owens, formerly IMPATH's Senior V.P of Operations, is taking a sabbatical in Southern California. • Paul Esselman, formerly IMPATH's Senior V.P. of Sales and Marketing, is now **LipoScience Inc.'s** V.P. of Sales.

***That's all the insider intelligence for this report. Look for the next briefing on Monday, May 9, 2005.***

*PREVIEW #6*

## EXECUTIVE WAR COLLEGE

May 3-4, 2005 • Astor Crowne Plaza Hotel • New Orleans

### Building a Financially-Viable Molecular Program

Growing numbers of hospital laboratories show interest in offering molecular tests to clinicians, but are deterred by questions of reimbursement, complexity, and other uncertainties. Beaumont Health System's successful clinical molecular testing program provides useful insights about essential "do's and don'ts" when establishing such tests in community hospital settings. Gain practical wisdom on topics such as: knowing when the time is right to set up and offer such tests, negotiating effective contracts with molecular vendors, and educating clinicians about ordering molecular tests.

***Full program details available now!***
*visit darkreport.com*

# *UPCOMING...*

- ***CDC's "Destruct" Order for CAP's H2N2 Flu Proficiency Test Kits: Key Lessons Learned from this Significant Blunder.***
- ***Commentary on the Current "Crime Wave" Within the Laboratory Industry.***
- ***Medicare's Competitive Bidding Demonstration Project: Who's Watching Out for the Lab Industry?***

*For more information, visit:*
**www.darkreport.com**