EMBARGOED UNTIL DELIVERED, approx 6:30 pm 1/25/11

White Collar Crime in 2011: The Martin Act, Cybercrime, and Beyond

Cyrus R. Vance, Jr.
District Attorney, New York County
January 25, 2011, New York City Bar Association

Thanks to my friend Harlan Levy for that generous introduction, and thank you to the Council on Criminal Justice for inviting me to speak here tonight. As a former member of the Council, I am particularly honored to give this presentation. In fact, one of the last times I spoke in this room was at the Council's criminal justice retreat in 2008, before I was DA, about the role of the modern prosecutor.

Now that I am District Attorney, I think every day about the prosecutor's role. In Manhattan, the primary role of the District Attorney has been and will continue to be ensuring the safety of the public, in their homes, on the streets, and in their daily lives. In fact, I think it is fair to say that never in my office's history have we had a more sophisticated understanding of the street crime problem in Manhattan, nor been more proactive in addressing that problem. But as passionate as I am about our battle against violent crime -- as well as many other things of interest to the City Bar, such as re-entry and alternatives to incarceration -- a discussion of our initiatives and our Office's advances in those areas in the past year will have to await another day.

What I want to talk to you about today, and to put into historical perspective, is the Manhattan DA's Office's continuing leadership role in the battle against white collar crime. All of my three immediate predecessors – Tom Dewey, Frank Hogan and Robert Morgenthau – implemented new strategies to deal with the increasingly complex economic crimes that threatened the public during their tenures. And like my predecessors, I am mindful of the staggering economic costs that white-collar crimes exact from the law-abiding public.

It is hard to believe that the term "white collar crime" is barely 70 years old. It was coined in 1939 by a sociologist, Edwin H. Sutherland, who defined it as "crime committed by a person of respectability and high social status in the course of his occupation." Sutherland chose to define

the phrase in class terms — "high social status" — rather than the definitions we might use today, which are based more in descriptions of the crimes than the people.

And like my predecessors, I recognize that the very legitimacy of law enforcement depends upon demonstrating that the powerful, the wealthy, and the privileged enjoy no immunity from prosecution as a consequence of their status. And so, for the past year I have been working with a dedicated staff of highly experienced lawyers and investigators to continue the tradition of innovation started by those who came before me.

What has come to mind as I take on this task is the old expression that "everything old is new again," both in terms of the crimes we're seeing and the investigative techniques we're using.

People in positions of trust are still embezzling from their companies and their clients.

Investment advisors and brokers are still misrepresenting the nature of investments to make a fast buck.

Companies are still manipulating their balance sheets to deceive investors and prop up their stock prices.

But these recurring themes don't tell the whole story of the challenges confronting the Manhattan DA's office in 2011. As the very nature of our economy has changed dramatically over the past generation, white collar crime has changed dramatically as well – and so must our law enforcement strategies evolve to keep pace.

What I intend to do is split my remarks tonight into three parts: First, I will fill you in on some of our Office's innovations in the area of white collar crime enforcement, both structural and substantive. Next, I'd like to talk about an important enforcement tool that the Manhattan DA's office has been using for decades – the Martin Act – and how we will apply that tool to securities and other frauds today. And finally, I'd like to tell you about a category of frauds that is indeed new: identity theft and cybercrime. I have said many times before that the internet is the crime

scene of the 21st century. Tonight I'd like to talk to you about what we're recovering at that crime scene.

White Collar Crime

Let's start with a bit of history. Enforcement of sophisticated frauds and securities laws has traditionally been a local law enforcement function in New York. District Attorney Joab Banton was bringing securities fraud cases in the 1920s, and in 1938 Thomas Dewey prosecuted Richard Whitney, former president of the New York Stock Exchange, for stealing from clients of his securities firm. That same year, District Attorney Dewey established a specialized Frauds Bureau in the Manhattan District Attorney's Office.

Today, that historic Frauds Bureau has been absorbed into our Major Economics Crime Bureau, which we created last April. We created that new Bureau because I came to see the interrelationships among a wide variety of white collar prosecutions that had been handled in diverse units previously scattered throughout my Office, and realized that by joining those teams under a single leader we would achieve practical and strategic advantages.

The new bureau is composed of about 30 Assistant District Attorneys and nearly 40 staff; and to head the bureau we were fortunate to attract Richard Weber, an accomplished former federal prosecutor who headed the national Asset Forfeiture and Money Laundering Section of DOJ, and who moved here from Washington to help us in our effort.

His focus and mine has been to continue building criminal cases that profoundly impact the diverse elements of our financial systems. Securities, commodities and investment fraud are a major focus, as are mortgage fraud and financial institution fraud.

Consolidating these functions within one unit capitalizes on a great strength that we in local law enforcement have long enjoyed, particularly here in Manhattan, but which I doubt is fully appreciated by the public: our broad reach into the community we serve. Our office last year handled more than 100,000 filed criminal cases. While most are not complex fraud cases, it is a

huge number and, in fact, numbers more than all the criminal cases filed by the Department of Justice nationwide. NO other prosecutor's office handles the volume and breadth of cases that we do in the Manhattan DA's office.

This is important because major fraud cases can come from anywhere. Many of you no doubt know about a local sales tax investigation that the Manhattan D.A.'s Office handled several years ago. The Office learned of a corporate executive who bought art works, and schemed to avoid paying the local sales tax on his purchases. That corporate executive was Dennis Kozlowski, and what began as an investigation of sales tax evasion mushroomed into the Tyco prosecution, one of the most significant corporate fraud cases in our Office's history. And by the way, lest you wonder whether criminal prosecutions can act as an effective deterrent to crime, statistics show that in the years following the Tyco prosecution, state tax revenues increased by 85 million dollars, a phenomenon the New York State Tax Department has referred to as the "Kozlowski Bump." The lesson from this prosecution is clear, and in training our assistants, we stress that any case that walks in our door, no matter what the initial subject matter, can potentially lead to a significant investigation, quite possibly in areas far afield from the original complaint – and this is especially true in the kinds of white collar cases we will be speaking of tonight.

And just as it is important to connect the dots internally, and forge ties across diverse units within my Office, we have also, over the past year, strengthened and in some cases forged new relationships with outside agencies like the SEC, the CFTC, FINRA, the Federal Reserve Bank of NY, and the Depository Trust & Clearing Corporation. Just this past fall, the Manhattan DA's office conducted its first ever banking symposium, which attracted nearly 400 participants from industry and enforcement. The event, hosted by the Federal Reserve Bank of NY, brought together all of these agencies I mentioned and more with representatives of the banking industry, in an effort to better cooperate and both solve crime and stop it before it happens. And this cooperation is yielding results: this past September, we announced indictments in a large international cybercrime ring in a case that arose from a joint cooperative investigation involving my Office, the FBI, and the U. S. Attorney for the Southern District. I look forward to many more opportunities for such fruitful cooperation in the future.

The Martin Act

In emphasizing the unique role that my Office has to play in meeting the challenges of sophisticated fraud in a 21st Century economy, I will start with the Martin Act; how we have used it and how we will expand its use. The Martin Act, the New York State law under which we prosecute securities fraud, was originally enacted in 1921 – 13 years before the federal act forming the Securities and Exchange Commission – and, indeed, 18 years before the term "white collar crime" was first coined by Professor Sutherland. The Martin Act was intended as a broad grant of authority to investigate and prosecute, as the Court of Appeals famously stated in 1926, "all deceitful practices contrary to the plain rules of common honesty." That judicial construction makes the Act sufficiently flexible to prosecute a broad range of frauds.

The Martin Act is a false statement statute, not just a fraud statute. To lie or deceive someone in the offering of securities — no purchase or sale is necessary — violates the law.

This past year, using the Martin Act, we've prosecuted
large-scale Ponzi schemes, such as our recent indictment of a foreign national, who enticed investors and friends into a multi-million dollar Ponzi scheme by falsely claiming that he was a close member of the Chimay royal family of Belgium with access to royal family money. We've also recently used the Martin Act to charge fraud in connection with investments in gold coins, and to file charges against those who gave friends and family millions of shares of illegal issued stock in a scheme to steal more than $60,000,000; to name just a few.

These are just a few examples of the Act's traditional use. My focus is on its future and broader application. In the coming year, in part because of new relationships with enforcement partners and a proactive approach, I expect you will see the Martin Act as a criminal enforcement tool in prosecutions of:

- investment frauds and Ponzi schemes involving investment funds
- investment frauds using privately-held companies
- fraud schemes that actually *target* broker-dealers
- manipulation of commodities and commodities futures

- insider trading in securities and commodities.

I believe the Martin Act has never been more relevant. In recent years, our entire nation has become painfully aware of the devastating toll on our economy that results when widespread mistrust infects financial markets. Without trust, quite simply, our economy ceases to operate. No bank will close on a loan when no one can rely on the truthfulness of the representations in the application. No investor will purchase a financial instrument when there is no assurance that the security that backs it is real. And that is why we must continue to uncover those deceitful practices that the Martin Act has outlawed for the better part of a century, those that are "contrary to the plain rules of common honesty."

But the flexibility of the Martin Act, and its utility in the battle against criminal fraud, is marred by its overly lenient penalties. The highest level crime, which at its simplest involves intentional false statements resulting in a loss over $250, is only a Class E felony, with no minimum term of imprisonment regardless of the amount of money involved. Thus, a broker who fraudulently deprives one customer of $500 is subject to the same penalty as a high-level market manipulator who deprives the investing public of hundreds of millions of dollars. And in either case, a state court judge would be authorized to impose a non-incarceratory sentence.

This year, as part of my legislative proposals, I will be calling on the Legislature to reform the Martin Act, to make it even more powerful in the battle against fraud, by conforming the penalties for different loss amounts to those in the current Grand Larceny statutes and by increasing the statute of limitation. Thus, the small-time broker who defrauds his customer of only $2,000 would be subject to the E felony maximum of 1-1/3 to 4 years, while the sophisticated manipulator or perpetrator of a large-scale accounting fraud would be subject to a prison term of up to 8- 1/3 to 25 years, and a mandatory minimum state prison term of 1 to 3 years.

Interestingly, I am not the first District Attorney to complain about the Martin Act's bite: in 1925, Manhattan DA Joab Banton complained to the New York Times about the first iteration of the law, which then lacked criminal provisions and granted immunity to anyone who testified in

connection with securities investigations: Banton noted, "It is said that the Martin law has teeth. It has, but they are an ill-fitting set of false teeth." He went on to ask the Legislature to amend the law to "make New York safe for the investor." That's what I will be asking the Legislature today, as well.

While it is true that everything old is new, we are using brand new tools of 21st Century law enforcement I would like to discuss with you. One is our use of the provisions of the federal Bank Secrecy Act and its guardian agency, FinCEN. Thanks to the sophisticated FinCEN database system, our Office receives reams of Suspicious Activity Reports, better known by the acronym SARs, every week. Financial institutions are required to file these forms when they detect suspicious activity, even where that activity does not in itself run afoul of any other law.

These reports are the raw material out of which major cases can be made, but as with so much in law enforcement, the challenge is to make sense of a large mass of information. To that end, we have created a SAR Action Team to search for actionable SARs on a daily basis. Analysts spend hours each week conducting these searches for crimes and trends in areas that include Ponzi schemes, unlicensed money remitters, international money laundering, securities and other investment fraud, and mortgage fraud. If a SAR warrants further investigation, a team of ADAs and paralegals is assigned, and works with investigators from my office, as well as outside partners like the IRS Task Force and the New York High Intensity Financial Crimes Area – better known as the HIFCA.

The goal of our SAR Team is to find cases and to investigate aggressively those matters that will result in the disruption and dismantling of criminal operations. Our prosecutors and analysts communicate directly with banks to enhance our cases and to give banks the information that they need to assist us.

Let me give you just one example of why SARs are an invaluable tool. An analyst in my Office, during one of the routine reviews I've just told you about, came across a SAR and referred it to an assistant district attorney to investigate. That investigation led to the successful prosecution of a hundred million dollar mortgage fraud ring – one of the largest mortgage frauds uncovered

since the recent economic crisis – and led to convictions of over 20 individuals who lied, cheated and stole from dozens of financial institutions. The lead defendant in that case was just sentenced to 8 1/3 to 25 years in prison.

That mortgage fraud case, in which we secured a state racketeering conviction last year, is just one example of how our case work continues unabated in the broader white-collar fraud area. In the past year, since I became District Attorney, we announced a deferred prosecution agreement with Barclay's Bank in the amount of $149 million, which funds brought to approximately $400 million the amount that our office has returned to the City and State of New York IN THE LAST YEAR. In the area of tax fraud, we secured the convictions of 28 individuals for tax crimes and brought in $25 million in tax restitution for the State and City of New York. And in another case, we successfully prosecuted medical professionals in a no-fault fraud mill using the novel theory that an entire no-fault clinic and all of its insurance claims were fraudulent because the conspirators concealed the true ownership of the clinic from the insurance carriers.

These kinds of highly visible results have an added pay-off: they encourage law enforcement agencies, financial institutions, victims, and whistle-blowers to bring more cases through our door. My hope is that over the coming months and years, you will see these efforts bear fruit as we go after ever more sophisticated financial crimes.

Cyber-crime

And a primary 21st Century example of this is in Cybercrime.

The globalization of the internet has brought growth to our economy and an ease and immediacy to our communications. And yet, at the same time, it has allowed for the creation of an unintended intimacy – a false intimacy — with people about whom we know nothing more than their email address. It also provides a dangerous set of tools for the criminally-inclined not only to work their way into our personal lives, but to threaten our society on an individual and institutional basis.

In fact, cybercrime and its close cousin, identity theft, are among the fastest growing crimes in the country. Some Manhattan police precincts report that identity theft is their most frequently

reported crime. Ironically, while incidents of violent crime have largely decreased in New York, prosecutions for cybercrime and identity theft have grown at an alarming rate – up about 50% in the past five years.

We in law enforcement broadly define cybercrime as any crime where a computer or the internet is used to commit or conceal a crime. Any number of cases can have a cyber-element to them: Computers and corporate computer systems are often targeted by malicious hackers who surreptitiously install software, allowing them to destroy, damage, or steal information from home or office. The malicious software – or malware – can be used to infiltrate businesses and wreak financial damage.

More personally, computers can be used as instruments of stalking or harassment via e-mail or social networking sites. They can also be used to traffic in child pornography on the internet.

In the identity theft arena, hundreds of thousands of credit card numbers are sold via the Internet on underground sites. Often, those account numbers were stolen via computer intrusions or other high-tech methods involving the use of a computer or the internet.

Finally, the internet is fraught with scam artists trying to trick people into giving them money or merchandise. These scams run from the small time bait-and-switch schemes as you might see on Craigslist, to sophisticated phony websites that are set up to look like genuine sites, such as major banks or the Internal Revenue Service.

This is a growing threat, and it is as frightening as it is real. To move aggressively to combat this threat, last year we created the Cybercrime and Identity Theft Bureau. The bureau is now composed of 10 ADAs who spend all of their time on these matters, and about 70 who spend at least part of their time.

The Cybercrime Bureau has two primary responsibilities. First, it is tasked with providing supervision and expertise for 200 to 300 new identity theft cases *per month*. The overwhelming majority of these cases come to us from arrests by the NYPD. They are handled by the 70

designated ADAs within our Trial Division, who receive special training and handle these cases in addition to their regular duties. We also track these cases and find important links between them, which can be an invaluable tool in discerning criminal patterns and typologies, and in identifying criminal organizations that would otherwise go undetected.

Second, our full-time and other major case ADAs conduct intensive, long-term investigations and prosecutions of national and international criminal organizations as part of our Investigation Division. This mission includes developing long-term malware, hacking and intrusion investigations as well as sophisticated cyber-frauds.

What is striking about many of these cybercrime and identity theft investigations is that major investigations often begin as local arrests having nothing to do with cybercrime. In one case, we had a pattern of thefts from lockers in a gym. As we investigated, we learned that the personal information culled from those thefts were used in a vast identity theft ring. In other instances, cases began as summary arrests of a person presenting a single forged check at a bank window. Investigation revealed that the check was the tip of a large iceberg of organized identity theft and fraud.

There is no way to detect these patterns other than the laborious task of sifting through individual cases as they come into our Office. Every morning, a supervisor in our Cybercrime Bureau reviews every case that was written up in our complaint room the day before. Where the allegations suggest that identity theft may be a motive, or where we suspect that cybercrime may be involved, they speak to the assigned prosecutor, to begin to explore the potential outline of the underlying criminality. As I say, it is a painstaking task, but we in the District Attorney's Office have access to a nearly limitless store of raw intelligence. Our task is to devote the hard work necessary to make sense of it. And time and again, that hard work has paid off.

This past September, for instance, we announced the indictments of 36 individuals for their participation in several large-scale international identity theft and cybercrime rings that stole

hundreds of thousands of dollars from 34 separate corporate and individual victims in the United States. The victims' bank account information was obtained through the use of malware, surreptitiously planted in victims' computers, enabling accomplices overseas to steal personal identification information relating to the victims' bank accounts. This information was then used to transfer money from the victims' bank accounts into the bank accounts set up by these defendants.

The 36 defendants, foreign students from the Russian Federation, Ukraine, Kazakhstan and Belarus, who were in the United States on Exchange Visitor Visas, are charged with opening bank accounts at JP Morgan Chase Bank and other financial institutions for the purpose of receiving fraudulent transfers from identity theft victims' bank accounts. We previously arrested and charged 19 other individuals with related crimes.

But it is not just hackers, or cyber-thieves operating on remote shores, who are pirating stolen information. A large and growing problem is what we call "insider identity theft," in which trusted individuals within large companies or banks acquire confidential information and sell it in an organized way. That information is in turn often used to manufacture counterfeit checks or credit cards.

For example, in a case that concluded last year that we dubbed "Paper Chase," the office filed indictments against 18 of the ringleaders of a well-organized criminal conspiracy. The defendants paid tellers in major New York Banks to provide photocopies of legitimate checks, along with personal information belonging to approximately 500 identity theft victims. The ringleaders used that information to manufacture thousands of counterfeit checks. By fraudulently cashing and depositing these counterfeit checks, the defendants stole millions of dollars from victims including Equinox Fitness Club, Harlem Children's Zone, Diane Von Furstenberg, Madison Square Garden, the New York City Board of Education, and even the Bronx Property Clerk of the New York City Police Department.

The list includes some very sophisticated victims, and this is another trend we're seeing. Even major corporations become victims when identity theft rings use stolen credit card information to purchase millions of dollars of merchandise, which they then convert into cash using a very old-fashioned technique – fencing.

In short, no one – no individual, and no institution – is immune from these kind of crimes. And so, one important function of our Cybercrime Bureau is to alert the public to the steps they must take to ensure that their computers are secure and their personal information safe.

That is an enormous challenge, and there is no turning back: the new economy simply demands the free flow of goods, money, credit, and information. Keeping all of those things out of the hands of sophisticated criminals is, in this free environment, a demanding task. Every time we bring down a major cybercrime ring, it seems the criminals develop new and more sophisticated techniques to try to evade us.

And so we are not shy about using all of the tools available to foil them. We increasingly seek court orders allowing us to search hard drives and obtain records from internet service providers, and we continue to seek warrants allowing us to eavesdrop on telephones, texts, and emails. And we are similarly aggressive in partnering in appropriate cases with agencies that can help us dismantle major criminal enterprises. We have established, for example, a close working relationship with the United States Secret Service and its Electronic Crimes Task Force, and for the first time we have also been working closely in the appropriate case with the FBI and its new New York cybercrime division

Conclusion

It has been an honor and a pleasure to speak with you tonight. I am happy to take questions, but before I do I would like to leave you with one thought, in line with my theme of "what's old is new." As you've heard, we are being proactive like never before, and we expect that that will give us a head start on some of the crimes and criminals that we will be going after. But no

amount of intelligence gathering can supplant responsible lawyers like those in this audience, when it is in their clients' interest, advising those clients to report crime to the District Attorney. Indeed, last year for the first time in the history of a local prosecutor's office, we issued a policy on charging organizations, modeled after the federal policy, which explicitly rewards companies for cooperating. And we mean it – nothing is more important to us than self-reporting and full cooperation by companies who want to do the responsible thing.

And so I leave you with a plea for your help in helping us fight crime in the 21st century. We have several different hotlines on the website, but I invite you to call me or my executive staff directly. I can't guarantee the outcome, but I can guarantee a fair shake and an aggressive, proactive, and fair staff of prosecutors.

Thank you again for having me.