Bank Security: Own the Night

How financial institutions can apply the Broken Windows Theory of Policing to prevent criminal activity and stop losses due to fraud

Tom Leuchtner, *Director Financial Crime Control Solutions*, Wolters Kluwer Financial Services
Tony Kaus, *Senior Consultant Financial Crime Control Solutions*, Wolters Kluwer Financial Services

Introduction

Chief Security/Risk Officers (CSO/CRO) and those working in Fraud Mitigation, Loss Prevention and Operational Risk Management for financial institutions are dealing with a new era of cybercrime ushered in by the e-banking revolution. Often facilitated by insiders, cyber attacks use computer viruses and malicious code (malware) to siphon off millions of dollars every year in fraudulent wire transfers, Automated Clearinghouse (ACH) transactions and other unauthorized account activity.

An effective financial crime control program prevents such fraudulent activity by detecting behaviors that typically precede an attack and, at the earliest stage, disrupting the cycle of crime that results from potentially dangerous relationships between employees, customers and outside criminals. The constant presence of an automated sentry disrupts criminal activity, dissipates threats and, most importantly, enables the deterrence of future criminal attacks. This strategic approach to fraud prevention focuses on precursor behavior patterns and transactions, much like the "Broken Windows" approach to policing pioneered by the New York City Police Department in the 1970s. It is a strategy that breaks the cycle of crime and effectively mitigates risk.

This paper explores aspects of the "Broken Windows Theory of Policing" that have been successfully implemented nationwide. The paper points to effective lessons learned from the Broken Windows approach that are applicable to today's world of cyber-crime. By applying the Broken Windows theory to anti-fraud and loss prevention strategies, financial institutions can signal a "police presence" that maintains order and promotes integrity in the workplace. The paper outlines clear strategies and actions that can help in fraud mitigation, loss prevention and operational risk management. Further, this paper investigates how real-time monitoring and reporting can provide actionable intelligence for the interruption of activities and behaviors that are the pre-cursors to financial crime, effectively disrupting fraudulent schemes before they come to fruition.

Wolters Kluwer
Financial Services

Origins of Broken Windows Theory

Police foot patrols dispatched to crime-ridden neighborhoods in the mid 1970s adopted the motto, "We own the night,"[1] when their crackdown on petty crime made city streets safer. Operating on the theory that just one broken window can send the signal that no one is watching, police maintained order by enforcing laws against vandalism, littering, trespassing, disorderly conduct and other quality-of-life crimes. The so-called "Broken Windows" theory of policing, popularized by a 1982 article in *The Atlantic*,[2] has since been tested and proven effective in cities throughout the United States.[3]

In the mid 1990s, the New York City Police Department (NYPD) added the dimension of comparative statistics (CompStat) computer analysis to map crime statistics and guide enforcement activity surrounding more violent crimes. With CompStat statistics to guide their rapid response to violence, the NYPD effectively cut crime in half.[4] To this day, weekly CompStat meetings inform the tactical law enforcement and strategic deployment of specialized units by New York's Finest. This crime prevention strategy has now been adopted by cities nationwide[5] — perhaps most notoriously in Baltimore, Maryland, as seen on HBO's The Wire.[6]

Combined with the Broken Windows approach to order maintenance, CompStat methods have fared well over time. New York Police Department figures reveal that in the decade from 1993 to 2003, the total number of reported crimes for the seven major crime categories declined an unprecedented 66 percent.[7] Today, the overall level of crime in New York City is at its lowest point since 1963, and the city is ranked as the safest of the 10 largest U.S. cities.[8] Elsewhere, metropolitan areas of all sizes cite CompStat as a success factor in reducing violent crime. For example, the Daytona Beach Police Department (DBPD) has documented a 19 percent drop in crime since implementing CompStat in 2006; in a survey of other police departments, DBPD Lieutenant Charles Fordham noted agencies in Boston, Miami, New Orleans and Newark reported comparable results.[9]

If there is a lesson to be learned from Broken Windows theory and practice, it is that an aggressive police presence not only deters criminal activity but also disrupts behavior patterns that eventually lead to more violent crime. It is a proactive approach that relies on timely and accurate information about where criminal activity has occurred in the past—and where it may occur in the future. It also includes clear communication that enforcement is underway, providing effective deterrence by telling the criminals that a new systematic and preventative approach in each neighborhood will identify any suspicious activity, and the perpetrators will be dealt with by the strongest means available.

In the banking industry, there are comparable signature behavior patterns and activities that precede financial crime. Violating login policies, excessive account inquiries, probing account credentials and staging dormant accounts are all precursors to fraudulent activity. Financial institutions can look for these "broken windows" to detect and prevent fraud.

Broken Windows in the Banking Neighborhood

Incidences of cybercrime have grown at an alarming rate, despite increasingly sophisticated security measures in the financial industry. Criminals working both inside and outside the system have escalated their attacks by keeping pace with security updates and targeting institutions that have less sophisticated anti-fraud systems. In the nine-year period from 1997 to 2006, annual fraud losses escalated from $512 million to $11 billion, according to the American Bankers Association.[10] The ABA's most recent Deposit Account Fraud Survey found that in 2008, check-related losses alone rose to $1 billion, and losses from debit card fraud reached $788 million.[11] Fully 80 percent of banks reported having check fraud losses in 2008.

As a result of these financial losses, many institutions have suffered significant degradation of their reputation, brand loyalty, customer satisfaction and trust, and investor confidence. Unrecovered funds also degrade profitability, whether through slow leaks of small losses or one-time rip-offs that go undetected until after the fact. This has put severe pressure on boards and operational managers to account for what these losses mean to the institution. Those responsible for tracking six- and seven-figure losses are often at an extreme disadvantage, left without a viable audit trail or the forensic evidence to uncover the source of the leaks, let alone the ability to recover even a small percentage of the lost funds.

Fraud has become more pervasive in large part due to the growth of electronic banking, which includes Internet banking for consumers and the higher risk of access through electronic cash management and payments systems. Although electronic banking has been around for some time in the form of automatic teller machines and telephone transactions, it has been transformed by the Internet; e-banking has lowered the cost of a typical customer transaction from about $1 at a brick-and-mortar bank to about $.02 online.[12] As early as 2001, banks with transactional websites accounted for 90 percent of national banking system assets, putting a significant portion of the nation's financial assets at risk of cyber attack.[13] Increased competition has created numerous additional pressures on banks, such as:

- Merging banks, which can lead to multiple legacy systems running simultaneously without effective access and monitoring controls;
- Adding new products too rapidly, preventing thorough evaluations of new products' operational risk; and

- Selling existing products too aggressively, which can give rise to sales gaming schemes and lowering risk thresholds for customer acceptance.

Reliance on the Internet to provide banking services has made security and system availability a central focus of risk management. Anti-fraud programs have been built around Customer Identification Processes and best practices in case management to harden financial institutions against attack.[14] However, the outcome of existing countermeasures tend to lean toward detection, not prevention, proving ineffective in abating financial crimes committed by organized co-conspirators. Nearly one half of all fraudulent activity involves collusion between insiders and outsiders.[15]

While banks have been introducing a broad line of online services, criminals have been honing attack strategies to circumvent the safeguards that are in place. The typical automated anti-fraud solution employs transaction monitoring to detect historical patterns and predict potentially criminal activity; yet these systems do nothing to deter suspicious behavior as *it occurs*. Therefore, large-scale, cyber attacks can net hundreds of thousands of dollars and go undetected until after the criminal activity has effectively accomplished its goal.

By comparison, small-time fraud, when identified, often goes unprosecuted—further encouraging criminal activity. A bank's own employees may continue fraudulent activity knowing that financial institutions typically fire miscreants without prosecution to avoid negative publicity. In loan processing, for example, a fraudulent event may be as simple as a cash-strapped loan officer who made fake loans. Once discovered, such a perpetrator may be quietly terminated and blacklisted from future employment in a financial institution. This is especially true when the individual can make some restitution and cooperates by describing the steps used to perpetrate the crime.

Anti-Fraud and Accountability

Using the CompStat Approach to Gauge Performance

In 1994, as part of New York City Mayor Rudy Giuliani's crack down on crime, Police Commissioner Bill Bratton instituted CompStat, a comparative statistics approach to mapping crime, identifying patterns and targeting enforcement. CompStat is credited with bringing down crime by 50 percent.[30] Since then, CompStat-style policing has been adopted in cities from Raleigh, N.C., to Ann Arbor, Mich., with double-digit success in crime reduction.[31]

The hallmark of the CompStat strategy is accountability. From officers on foot patrol to the precinct commanders, police assume responsibility for anticipating and preventing crime in their jurisdictions. The CompStat approach includes these key elements:

- **Weekly Reporting.** Crime statistics are updated and mapped by location, type and time.
- **Interrogative Briefings.** At weekly CompStat meetings, bosses probe underlings—in front of their peers—about crime trends and what is being done about them.
- **Strategies and Tactics.** Crime trends, deviations and anomalies inform department counter-measures.
- **Leadership Presence.** Decision-makers participate in weekly meetings and immediately commit resources.
- **Enforcement Discretion.** Officers are given latitude to determine the best tactics for reducing crime.
- **Performance Charting.** Departmental and individual performance is measured by the numbers of apprehensions and specific crimes (murder, rape, robbery, etc.).

NYC's CompStat initiative won the 1996 Innovation in Government Award from the Kennedy School of Government.[32] Today, it is still used to critically assess the NYPD's patrol and investigative operations.[33]

As an aggressive management strategy that holds front-line forces accountable for lowering crime statistics, CompStat can be adapted by financial institutions that have access to detailed statistical reporting tools, such as *Wiz* Sentri: Anti-Fraud. Using real-time reporting capabilities to establish trends and set performance standards can significantly improve the success rate in fraud prevention and prosecution.

The CompStat approach is a game changer. As a Raleigh police captain told The New York Times, "It is a paradigm shift like I've never experienced before. It's the difference between responsibility and ownership."[34]

As "Broken Windows" authors James Wilson and George Kelling reported, such crimes are the inevitable result of disorder. Malcolm Gladwell, author of *The Tipping Point*, put it this way: Minor, seemingly insignificant crimes are the tipping point for more severe criminal activity.[16] On the streets of New York City, vandalism can escalate criminal activity to the point of felony. In banking's bad neighborhood, uninterrupted precursors to fraud can lead to multi-million dollar cyber attacks. Like the first broken window in a neighborhood, financial fraud sets off a chain of events that result in significant losses to an institution's brand, reputation, competitiveness and profitability.

Accepting fraudulent activity as a manageable cost of doing business is not only bad business policy, it is unacceptable in today's society.[17] Institutions that have been the unwitting instruments of fraud (such as when a bank customer's business account is targeted and emptied) suffer the ignominy of bad publicity and lost business. In *Corporate Resiliency: Managing the Growing Risk of Fraud and Corruption*, Toby Bishop and Frank Hydoski suggest that for companies to avoid the dire consequences of fraud, they must deploy strategies to assess, prevent, detect and respond to fraudulent activity.[18]

Policing the Electronic Banking Streets

A bank's "broken windows" are the electronic signatures of suspicious activity that precede criminal attacks. These signatures are the only visible sign that a crime is about to be committed. Violating login policies, excessive account inquiries, probing account credentials and staging dormant accounts are all indicators of impending fraudulent activity. For example, outsiders who hijack customer credentials and login to electronic banking systems may execute a series of small probing transactions before making a massive withdrawal. By comparing the real-time behavior and activities of various entities (such as customers, accounts and employees) to historical profiles of normal behavior for these entities, financial institutions can identify precursor behaviors and prevent serious crimes from happening.

The banking systems that are most vulnerable to fraud include deposit accounts, online banking, loans and payment systems. Industry wide, deposit account fraud is estimated to comprise more than 60 percent of all fraud attempts.[19] In a typical attack, cyber thieves target a networked computer that is used for initiating wire transfers or ACH transactions. They install malware on the computer via an e-mail message or booby-trapped website, and the malware monitors for and records the usernames and passwords necessary for online banking transactions. Using these methods, criminals can clean out an account in near real-time without ever triggering an alert. The malware has become so capable that it can compromise the most sophisticated security tokens and authentication techniques.[20] Some malware infects other malware, showing the sophistication and tenacity of the criminals responsible for these attacks. Moreover, these attacks have continued to escalate in recent months.

In the Broken Windows Theory of Policing, a strong police presence on city streets enforces the rules of law and order and effectively reduces criminal activity. Likewise in banking, systematic and visible oversight can deter insider fraud and detect outsider probes before they escalate. Without a proactive approach to security, internal fraud schemes typically go undetected for 24 months.[21] The standard security measures in practice today only identify an event after the fact, when less than 20 percent of funds can be recovered.[22]

To prevent losses, financial institutions can establish a "police presence" that provides real-time surveillance for the precursors to financial crime. A real-time enabled, automated anti-fraud solution continuously monitors the links between employees, customers and their accounts and flags abnormal activity for investigation before crime occurs. This type of system provides insight into what information is being accessed or changed, how often and by whom; as well as whether behavior and activities are within established norms.

There are many subtle indicators of potentially fraudulent activity. The best way to identify these indicators is to use technology capable of monitoring the network and information about related activity in real time. Financial institutions can use automated tools that will establish behavioral norms, or profiles, based on actual events. When behavior deviates from these norms, the abnormal behavior patterns are automatically flagged and prioritized for investigation. Responding to a credible alert, the financial crime control team can establish a presence in a disorderly branch office to quickly address the threat, or block an IP address and freeze an account before notifying authorities of an attempted cyber attack.

A key element of an effective financial crime control program is disrupting dangerous relationships between employees, customers and outsiders. The constant presence of an automated sentry disrupts criminal behavior, dissipates threats and deters future criminal activity. This proactive approach to fraud prevention and detection effectively mitigates risk, much like the "we own the night" attitude of police officers reduces crime in their jurisdictions.

Maintaining Order in Banking Hotspots

The Broken Windows Theory of Policing credited the "order maintenance" function of police patrols with keeping peace in the community. Order maintenance sends the message that no

misdeed will go unnoticed or unpunished.[23] But what gave officers an edge in their jurisdictions was the introduction of CompStat—the statistical reporting of crimes at street level. When NYPD introduced CompStat meetings to the police command structure, officers could quickly identify hotspots where increasing numbers of crimes were occurring on their streets. They could immediately take action and disrupt the momentum.

Likewise, while real-time monitoring maintains order in financial systems, it is the comparative statistical analysis and reporting that provides an edge for the financial crime control team. A sophisticated anti-fraud monitoring and reporting solution can more effectively assess current risks to the institution through detailed and configurable real-time reporting tools and case management dashboards. These reporting tools empower security operations to identify hotspots, predict behavior based on current patterns and take action to disrupt suspicious activities.

These analytical tools also provide the means to measure how well a financial institution is managing risk and enable identification of areas for continuous improvement. CompStat-style security delivers actionable intelligence for rapid response to stop fraudulent activity before monetary losses are incurred. In this way, financial institutions can move from merely detecting fraud after the fact, to actually preventing fraud. With the proper rules and reporting systems in place, order is maintained.

Apprehending and Prosecuting Fraudsters

Criminologists have documented that vigilance to stop crime before it happens is the most effective deterrent.[24] But when a crime is detected, prosecution must be possible. For whatever reason—lack of resources, limited proof or inadmissible evidence—many cases of financial fraud go unreported and unprosecuted.[25] Financial institutions require an anti-fraud solution that collects and preserves forensic evidence to support timely action and facilitate prosecution by authorities. A good automated anti-fraud solution protects the evidence chain of custody by electronically "sealing" the data packet to prevent tampering or corruption.[26]

In an automated network surveillance system, abnormal behavior patterns are flagged; network activity is captured, encrypted and digitally signed; and the chain of custody of the evidence is preserved so that action can be taken. At the same time, investigators are alerted to activities outside the norm, and real-time risk reports provide a prioritized list of probable fraudulent activities for investigation. Systematic fine tuning of analytics reduces false positives, minimizes disruption of legitimate activity, and improves the success rate for remuneration and prosecution, if warranted. *For maximum effectiveness, updating of the behavioral pattern matching and fine-tuning of the rules parameters should be a continuous process, not a single activity.* Because fraudsters keep pace with the banking community's continually evolving business operations, employing tools that facilitate the updating and fine-tuning of bank defenses is paramount.

Over time, the financial institutions can build a history of normal behavior patterns and statistical profiles, so the surveillance system becomes highly attuned to anomalies that are precursors to financial fraud. Security operations thus armed are able to repair these "broken windows" and assure stakeholders that the financial institution is in a "good neighborhood," where order is maintained and financial crime is kept at bay.

Next Steps in Building a Strategic Plan

The most vulnerable organization is one that assumes it is secure. U.S. organizations lose 7 percent of their annual revenues to insider abuse and fraud, according to the Association of Certified Fraud Examiners.[27] In the absence of an aggressive approach to fraud prevention and detection, most fraudulent activity is discovered by accident or anonymous tip.

To improve their odds, financial institutions can deploy an automated anti-fraud solution that sends a clear signal: The "neighborhood" is under surveillance, and criminal activity will be detected and prosecuted. With vigilance, there will be no more "broken windows" in the financial institution's banking systems. CompStat-style monitoring, analysis and reporting empower security teams to proactively reduce risk and prevent losses. The business case for investment in such anti-fraud resources is clear-cut. Industry reports confirm that anti-fraud initiatives can deliver up to an 800 percent return.[28] Specifically, TowerGroup estimates that every $1 financial institutions spend on anti-fraud technology reduces fraud loss by up to $8.[29]

Building a long-term strategy to protect your institution against fraudsters is not a simple task, nor is it easy. However, there are some near-term steps that can be taken to commence building this foundation. Commitment to reducing fraud and rebuilding customer trust in the banking system, and securing a profitable future in the face of an ever-changing competitive landscape are the strategic drivers. Wolters Kluwer Financial Services recommends the following steps in moving toward a strategic foundation for getting in front of fraud:

1. **Perform a Strategic Risk Assessment:** Target the single highest risk/highest cost area in the electronic banking segment. For most customers, this is the area of Treasury/Cash Management, Online Banking, Wire/ACH or Check/Remote Deposit Capture.

2. **Adopt a Cross-Channel Anti-Fraud System:** Utilize the target, high-risk area needs to drive strategic deployment. Adapt processes to the platform and train staff in its use, fine-tuning and response. This should dramatically improve investigator productivity.
3. **Leverage Investment in Other Areas:** Some at-risk areas may be stove-piped or not covered. The new system may replace existing check kiting or ACH/Wire fraud systems, or introduce internal fraud/compliance monitoring at a time of choosing that coincides with business planning. Other areas such as compliance (Red Flag/ID Theft, CDD, AML) and/or audit can also utilize the same modular approach to anti-fraud infrastructure.
4. **Gradually Migrate to Single Platform:** A single anti-fraud platform uses a common framework of data capture, analysis, alert management, reporting and case management. This enables the organization to employ a common research/investigation methodology, which leverages training opportunities by providing consistency across personnel and processes, and facilitates cross-channel and enterprise-wide functionalities.
5. **Capture Cost-Benefit of Enterprise Anti-Fraud:** Using a single anti-fraud platform consolidates vendor risk and reduces costs. Ongoing rationalization and reduction of IT investment and expenditure delivers improved ROI for each new system being monitored.

Working closely with your security and risk management teams, Wolters Kluwer Financial Services can help implement the best practice methodologies and software solutions recommended in this white paper. Our industry leading consultants can help your organization identify and secure critical gaps in fraud security to better mitigate the risks of financial crime. Through a proactive program focused on preventing, detecting and investigating criminal activity, your financial institution can mitigate the tremendous reputational, regulatory and operational risks posed by financial fraud.

Make the quantum leap from post-event detection to true financial crime prevention.

The potential for financial crime is higher today than at any time in history. Fraudsters have access to seemingly unlimited resources, can attack from anywhere, and often come disguised as promising new customers or trusted employees. They are dedicated to discovering your institution's vulnerabilities and exploiting them.

As transaction volume increases, fraud becomes more difficult to monitor. Every customer, employee and transaction represents potential exposure. You need to detect stolen and exchanged identities, systematic check kiting, insider collusion, wire and cash machine fraud, information leakage and much more.

A fraud prevention strategy protects your customers' finances and preserves your institution's reputation and bottom-line profitability. The *Wiz* Sentri™: Financial Crime Control solution seamlessly collects, sifts and archives all routine data traffic. By continuously applying a sophisticated set of "fraud rules" to each data event, the system identifies anomalous activity and behavior in real time, then generates coded analyst alerts.

By identifying the signals of impending fraud, *Wiz* Sentri empowers you to investigate potentially criminal interactions and pin-point the source using relationship-mapping capabilities, and screen-by-screen reconstruction and playback facilities.

Real-time evidence collection enables immediate intervention, systems access lock-down and perpetrator apprehension.

Wiz Sentri: Financial Crime Control's capabilities are unique in the market-place, enabling financial institutions to prevent fraud by continuously monitoring network activity. To learn more about how *Wiz* Sentri can help your institution embrace the power of real-time "policing" and prevent fraudulent attacks, call Wolters Kluwer Financial Services at 1.800.261.3111 or visit www.PCi*Wiz*.com today.

[1] Cole, David, "Broken Windows Theory of Policing," All Things Considered, March 7, 2000.

[2] Wilson, James Q. and Kelling, George L. "Broken Windows," The Atlantic, March 1982.

[3] "Bad Behavior Contagious, Study Finds," CBSNews.com, Nov. 21, 2008.

[4] Annenberg Public Policy Center of the University of Pennsylvania, "The Not-Quite Truth About NYC," FactCheck.org, Nov. 27, 2007.

[5] Dewan, Shaila K., "New York's Gospel of Policing by Data Spreads Across U.S.," The New York Times, April 28, 2004.

[6] Volk, Steve, "Usual Suspects," Philadelphia Weekly, May 30, 2007.

[7] Henry, Vincent E. "CompStat Management in the NYPD: Reducing Crime and Improving quality of Life in New York City," 129th International Senior Seminar Visiting Experts' Papers, Jan. 11-Feb. 9, 2005.

[8] Henry, "CompStat Management in the NYPD: Reducing Crime and Improving quality of Life in New York City"

[9] Fordham, Charles H. "The CompStat Concept in Addressing Crime," Florida Department of Law Enforcement: Future of Police Operations, May 2009.

[10] Kaus, Tony, Sr. FIU Consultant, Financial Intelligence Unit, Wolters Kluwer Financial Services, Phone Interview Jan 19, 2010.

[11] American Bankers Association, "2009 Deposit Account Fraud Survey Report," ABA.com, November 2009.

[12] Schaechter, Andrea. "Challenges of the 'E-banking Revolution,' " Finance & Development, Sept. 1, 2002.

[13] Schaechter, "Challenges of the 'E-banking Revolution' "

[14] Slitz, John. "Fighting Economic Crime with a Resolved Identity Platform," Journal of Economic Crime Management, Spring 2004, Vol. 2, Issue 2.

[15] Slitz, John. "Fighting Economic Crime with a Resolved Identity Platform"

[16] Gladwell, Malcolm. The Tipping Point: How Little Things Can Make a Big Difference. Little, Brown and Company (February 2000).

[17] Birch, Dave, "Window Pain," Digital Money Forum, July 14, 2009.

[18] Bishop, Toby J. F. and Hydoski, Frank E. Corporate Resiliency: Managing the Growing Risk of Fraud and Corruption. Wiley (May 4, 2009).

[19] Kaus, Phone Interview

[20] Resnik, William; Towle, Holly K.; Judy, Henry L.; and Mahoney, Sean P. "Wave of Online Banking Fraud Targeting Business," K&L Gates Newsstand, Feb. 10, 2010.

[21] The Institute of Internal Auditors, "The Importance of Strong Controls," Internal Auditor 2008.

[22] Cooper, Todd, VP/GM Financial Intelligence Unit, Wolters Kluwer Financial Services, Phone Interview Jan. 15, 2010.

[23] Wilson and Kelling, "Broken Windows"

[24] Wells, Joseph T., "New Approaches for Fraud Deterrence"" Journal of Accountancy, February 2004.

[25] Martin, Alyssa, "The Three Most Common Types of Fraud," Credit Union Magazine, Aug. 1. 2008.

[26] Leuchtner, Tom, Sr. Product Manager, Anti-Fraud, Wolters Kluwer Financial Services, Phone Interview Jan. 15, 2010.

[27] SmartPros Accounting, "ACFE: U.S. Companies Lose 5% to Fraud, $652B Nationwide," SmartPros Ltd., June 27, 2006.

[28] Holden, Tom, "Fair Isaac Fraud Detection and Risk Analysis," MTM Alliance, Feb. 6, 2009 ; "2008 Annual Fraud Report to the Legislature: Targeting Fraud and Abuse In Washington State's Workers' Compensation System," Washington State Department of Labor and Industries, February 2009.

[29] Garcia, Virginia, "Taming the Hydra: The Emergence of Enterprise Fraud Management in Financial Services," TowerGroup, June 2005 (as referenced by Durrett, Mark D., "The Costs of Data Security Breaches and Identity Theft," Covelight Systems, March 2006).

[30] Annenberg Public Policy Center of the University of Pennsylvania, "The Not-Quite Truth About NYC"

[31] Dewan, "New York's Gospel of Policing by Data Spreads Across U.S."

[32] Wikipedia contributors, "Mayoralty of Rudy Giuliani"

[33] City of New York Press Release, "Phil T. Pulaski Named NYPD Chief of Detectives," New York City Police Department, Oct. 8, 2009.

[34] Dewan, "New York's Gospel of Policing by Data Spreads Across the U.S."

Wolters Kluwer Financial Services provides best-in-class compliance, content, and technology solutions and services that help financial organizations manage risk and improve efficiency and effectiveness across their enterprise. The organization's prominent brands include Bankers Systems, VMP® Mortgage Solutions, PCi, AppOne®, GainsKeeper®, Capital Changes, NILS, AuthenticWeb™ and Uniform Forms™. Wolters Kluwer Financial Services is part of Wolters Kluwer, a leading global information services and publishing company with annual revenues of (2008) €3.4 billion and approximately 20,000 employees worldwide. Other prominent Wolters Kluwer brands include CCH®, Teammate, and SWORD.

Wolters Kluwer Financial Services
130 Turner Street, Building 3, 4th Floor
Waltham, MA 02453
Toll-free: 800.261.3111
Phone: 781.663.5333
Fax: 781.663.5335

Wolters Kluwer
Financial Services

To learn more visit www.PCi*Wiz*.com or www.WoltersKluwerFS.com.