Gone are the days when tracking a suspicious set of transactions was straightforward for the experienced anti-money laundering professional. Money was moved from one account and wired into another with clear origin and destination numbers, after which it might be moved again to other accounts or withdrawn.

What was once relatively simple is now becoming remarkably complex as banks continue to modernize with online services and alternative payment systems, including everything from prepaid cards, to mobile banking apps, to virtual currencies. This ongoing process of innovation is dramatically improving customer access and experience, but, at the same time, it is also opening new pathways for cyber criminals to infiltrate, steal, and cover their tracks on the money trail.

Earlier this year, a gang of hackers was found to have infiltrated more than 100 banks in over 30 countries. By using a “spear phishing” campaign, the hackers lured bank employees to unwittingly open deceptive emails, providing the hackers with access and the ability to insert malware that manipulated the banks’ software, accounting, and ATM systems. Over a two-year period, as much as $1 billion was siphoned directly from the banks, and the proceeds were layered into the hackers’ own accounts, in some cases using the SWIFT network.1

This is one of many examples taking place at the intersection of bank compliance and cyber security. It is a tangled web, as cyber criminals are using both traditional and alternative payment methods to aid illegal activities and mask identities while completing scams at light-speed. With this new breed of criminal, AML teams are facing their greatest challenges to date.

Regulators are keeping steady and aggressive watch over how well compliance teams are prepared to handle these new risks. Banks faced record fines and regulatory scrutiny of compliance programs in 2014, as U.S. and European banks paid nearly $65 billion in fines and penalties. 2 In addition, twenty of the world's biggest banks have paid more than $235 billion in fines and compensation in the last seven years for breaching a variety of financial regulations. 3
Enforcement and investigations are increasingly challenging for regulators who are grappling with how to regulate a changing market with growing risks spread across cyberspace and the financial services industry.

In June 2015, the New York State Department of Financial Services (NYDFS) issued its long awaited BitLicense—new regulations for all entities engaging in virtual currency business activity. Notably, the BitLicense rules require such institutions not only to have designated compliance personnel and the same kind of AML procedures that apply to institutions handling fiat currency, but also detailed cybersecurity procedures. That is a reflection of how intertwined cyber crimes and the financial system have become. NYDFS is pioneering this regulation, but other regulations will follow.

Regulators are poised to take the same rigorous approach to investigating bank cybersecurity procedures as they have done with AML. At a recent conference, Former New York State NYDFS superintendent Benjamin Lawsky described cyber crime as a "huge threat to our financial system" and said “You are going to see a lot of action around cybersecurity and the regulation in that area.”

With these new regulations and risks, how can AML teams effectively leverage information about cyber criminals and identify suspicious transactions that are anonymous, fast, and hidden within a vast expanse of other data?

Unfortunately, there is no quick fix to managing these challenges. It requires a new mindset to understand the risks and then restructure and test programs to meet those risks. As a start, all banks, regardless of size, need to answer the following questions:

- How do your cyber and AML teams share information?
- Do you have a robust transaction monitoring system that is independently validated at least once per year?
- Are you prepared to review volumes of historical transaction data if regulators require you to do so?

**Bridge the Cyber and AML Divide**

The nexus of cyber crime and the financial system raises the question: with cyber-enabled crime making the movement of money harder to trace, shouldn’t bank cybersecurity and AML teams work together? There is compelling evidence to suggest that these teams should be integrated, or even merged. Investigations of more traditional money laundering cases focus on account routing numbers. Cyber investigations focus on IP addresses and online traffic data. Merging internet data
analysis with traditional AML techniques can be a powerful weapon to combat financial crimes.

As criminals move swiftly across cyberspace, bank AML teams remain grounded with traditional tools that are sure to miss key indicators. Banks need to strengthen resources to fight this battle through cooperation between cybersecurity and AML teams that currently operate in silos with minimal communication.

Before the prevalence of online banking, security cameras and other physical identification strategies helped detect suspicious behavior and locate criminals. Today, the IP address is key to identifying anomalies. If multiple transactions are made in different accounts from the same IP address, this is a clear indicator of suspicious activity. Why would multiple people in one house use the same computer to open accounts and conduct transactions? Clearly, more information is needed.

Sharing IP information is one example of how the AML and cyber teams can better coordinate. For thorough monitoring and risk management, suspicious customer activity must be assumed to involve a data breach, while every data breach must be assumed to be a financial crime in the making.

Cyber crime frequently goes hand-in-hand with suspicious financial transactions. Bank accounts, credit card accounts, and ATMs are illegally accessed via “spear-phishing” emails or other “social engineering” ploys. Spear-phishing is when you receive an email that appears to be from an individual or business that you know, however, it is from criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC. Often, it takes an anti-money laundering mindset to detect the crime, or even to understand that a crime has been committed.

Transaction monitoring is a great place to start this integration. A typical assault on a bank starts with online customer data being stolen. But that data—account numbers, PIN numbers, social security numbers, debit and credit card numbers—has no value to the thieves until they can convert it into cash. This is classic money-laundering—now playing out online.

The AML team, having set up the rules and triggers that detect fraudulent transactions, can provide the cyber team with vital information about dates, times, dollar amounts, and the frequency of all sorts of anomalous activity. The two groups can then work together to cross-reference this information with any spikes in wire transfers, online purchases, ATM withdrawals, or other vulnerable banking activities. In this way,
information flowing from AML to cyber can help detect and prevent attempts to monetize stolen data.

But the information needs to go in the other direction as well. Whenever the cyber team detects a breach in the bank’s firewall, the AML team needs to hear the alarm. The sooner they know about the intrusion, the sooner they can raise alert levels and heighten scrutiny of suspicious transactions.

Both teams can then walk back the incident to identify any early indicators. What happened in the preceding days, weeks, or even months? Was money moved into or out of suspect accounts? Are there patterns to the suspicious behaviors? While AML works the transaction information, Cyber can track the IP addresses involved in the incident. Working together, the two groups can accomplish what neither could by itself.

Cybersecurity and AML need to work together. The silos must be torn down. Each group can add significantly to the effectiveness of the other, and there is simply too much at stake for them to continue working in isolation. What is needed is a freer, more streamlined sharing of information between AML and Cyber.

We anticipate that regulators will also be calling for more sharing and coordination. In the future, compliance officers might see a cyber version of the Suspicious Activity Report, with which all financial institutions are familiar. It would be up to regulators to determine specific triggers for a cyber-SAR, but the format that banks use today could be adapted to collect information such as attack indicators, targeted domains, and tools, techniques and procedures used by the suspicious transactors.

**Strengthen AML Processes and Procedures**

At a time when AML and cyber are converging, and regulators are stepping up their enforcement activity, financial institutions need to redouble their efforts to strengthen and improve the core elements of AML programs. “Fix it and forget it” simply doesn’t work. Compliance officers operate in a dynamic environment, and annual assessments are critical to ensure that AML and cybersecurity programs are keeping pace.

Each year, every bank should be doing an overall risk assessment of the different lines of business, their varied customer profiles, and possible exposures. Programs quickly become outdated if a bank is not keeping up to speed with new money laundering schemes and ways that criminals interact with financial institutions. AML teams also need to improve understanding of the newest emerging payment systems to understand
transaction patterns. Parameters must be reviewed and tested based on new risks to develop an effective set of rules to alert for suspicious activity.

As banks recognize the intersection of AML and cybersecurity, they will have a better ability to manage risks posed by new products, such as virtual currencies. Both teams must be involved in initial stages of the product development process. With a seat at the table, AML and cybersecurity officers can work together to help identify and implement proper controls. For institutions considering virtual currencies, it’s hard to envision banks not tapping the expertise of the AML and cybersecurity teams.

Checking the box is not enough. Programs need to be independently validated at least once per year. Enterprise-wide risk assessments should be conducted. Policies, procedures and KYC programs should be reviewed and tested, with extensive training for employees.

As banks move further away from in-person transactions, the criminals are quick to take advantage of more anonymity. It is imperative to modernize know your customer programs. The KYC programs of yesterday involved a checklist for bank branch employees to review with a customer that walked in the door, looking to open an account. Banks need to get to know and maintain contact with virtual customers. This requires training employees and evaluating progress on a consistent basis.

Get Smart on Data Analytics

Equally important to knowing your customer is knowing your big data. AML teams can’t make good decisions without a clear picture of the activity they’re monitoring and the risks associated with the data.

Banks hold on to massive amounts of data about customers. Customer information is critical to AML and KYC efforts, but holding too much outdated information poses a cyber risk. For example, many banks are holding on to information from former customers. This excess information poses an unnecessary cyber risk should that information be compromised. Banks are challenged to meet KYC requirements, but also have a firm understanding of what information is at risk for a cyber attack. It is critical for both AML and cyber teams to know the data and assess the risks involved.

Having the right analytics empowers compliance and cybersecurity efforts and minimizes the business disruption of scrambling to respond to challenging regulatory requests for specific data. A regulatory enforcement action can turn a compliance
department upside down with a request for specific information found in hundreds of thousands of transactions.

As a recent example, a bank was tasked with responding to regulatory enforcement action that required data analysis for approximately 75,000 merchants relating to a review of pre-paid debit card transaction activity for a period of 18 months. With powerful data analytics used by intelligence and law enforcement, the bank was able to identify potentially suspicious behavior by analyzing transaction patterns. This has resulted in substantive, large-scale investigative follow-up.

Detecting anomalies in a sea of data is a daunting task, but somewhat more daunting is preparing and normalizing data before it can be analyzed. After multiple mergers and acquisitions, banks typically find a patchwork of data formats. Different systems are merged and there is no uniformity of data points to monitor abnormalities. Now is the time to review the integrity of data, before a regulatory investigation occurs.

Once the data is normalized, that is when the analytics can launch into action to analyze activity including dates, transaction parties and financial instruments used. Having high integrity data and access to sophisticated analytics is critical to preventing and preparing for regulatory investigations.

Bank compliance officers should be prepared for these actions with regulator-approved methodologies to clean up problems in data, prepare it for sophisticated analysis and identify anomalous behavior. It is more than having the right tools. It is having a process for data ingestion, cleanup and developing a system where it will be possible to analyze and see the transactions and the trends over a given period of time.

**Modernizing AML**

AML is more complex at the intersection with cybersecurity. Compliance has entered an era of convergence, where silos have become risks, rather than just inefficiencies. Increasingly, financial institutions will see the advantages of a strategic, integrated approach to sharing information among their cyber and AML teams. Collaboration enhances their value to the institution, so it makes sense to bring them together in a coordinated way.

Compliance officers' roles have never been more challenging. They need to modernize and strengthen teams and programs to prepare for current and future uncertainties. The sophistication and diversity of criminal schemes will continue to grow.
Regulators have already acknowledged this intersection and will be increasingly focused on cybersecurity measures. Banks that share information, understand and prepare for risks, test systems and strengthen programs will be in the best position for success.

Endnotes
1http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab
2 http://www.wsj.com/articles/no-more-regulatory-nice-guy-for-banks-1419957394

ABOUT THE AUTHOR
Thomas Bock is Executive Managing Director and Head of the Anti-Money Laundering (AML) and Regulatory Compliance Practice at K2 Intelligence. He can be reached at tbock@k2intelligence.com.