Table of Contents

The Growing Threat of Enterprise-Class Fraud ......................... 1
Outwitting the Criminal Mind: The Challenges ......................... 2
  Fraudsters are more sophisticated than ever ......................... 2
  Fraud has evolved from rogues to rings ............................. 2
  The velocity of fraud has increased ................................. 2
  Cross-channel fraud is widespread – and difficult to detect ....... 2
  Rapid transaction processing makes it easy to grab and run ....... 3
  Financial institutions have to watch for the enemy within ......... 3
Where Many Fraud Programs Fall Short ............................... 3
  Fragmented and Reactive ........................................... 3
  Too Little, Too Late ..................................................... 4
  Ineffective Systems = Ineffective Investigations .................. 4
Layered Approach to Fraud Detection ................................. 4
  Layer 1: Endpoint-Centric – Secure the Points of Access ....... 5
  Layer 2: Navigation-Centric – Compare Website Behavior with What Is Expected .......................................................... 5
  Layer 3: Channel-Centric – Understand Users and Accounts by Channel ................................................................. 6
  Layer 4: Cross-Product, Cross-Channel – Correlate Activity and Alerts by Entity .......................................................... 6
  Layer 5: Entity Link Analysis – Gain Holistic Perspective of Related Customers ................................................................. 6
A Closer Look at Network Analysis .................................... 7
  Connecting the Dots ....................................................... 7
  Bottom-Up or Top-Down? ................................................... 8
Anatomy of a Credit Card Bust-Out ................................... 9
Enterprise Fraud Management in Action in Other Industries ...... 10
  Curbing Abuse of Government Assistance Programs .......... 10
  Detecting Underreporting or Abuse of Workers’ Compensation .. 11
Closing Thoughts ................................................................. 12
The Growing Threat of Enterprise-Class Fraud

The criminals are patient. Their business adopts a manufacturing mentality, where there is always work in progress – inventory on hand, waiting to be cashed in. They continuously create fraudulent identities, open accounts and do a little bit of activity in these accounts for a period of time. A year, two years, maybe five years. They set the pattern and get the bank comfortable with the account.

They ask for credit line increases, or the bank offers them. Bit by bit, the $1000 credit limit grows to $2500, then $3000 and eventually – given the consistent and seemingly trustworthy record of normal card use and payments – the limit might reach $20,000.

That's when the big transaction hits, and the fictitious credit card customer disappears – sooner if they think investigators might be on to them.

When fraudsters operate as well-organized enterprises with a work-in-progress mentality, there's a constant stream of available accounts ready to bust out. Financial institutions could continuously be at risk of being targeted by sophisticated “sleeper rings.”

The way these organized fraud rings operate today makes their activities difficult to detect with traditional, silo-based transaction monitoring systems. One system might flag a transaction as suspicious, but without a complete view of the customer’s relationships, the investigator could deem it innocuous. What if investigators could see the greater context around that suspicious transaction?

What if they could see that the account was linked in some way to another account? They might find that collectively the transactions are suspect, even if they appear normal when viewed in isolation. Imagine the power of having a holistic view of interconnections between accounts and transactions – not just for individual transaction channels and products, but across channels and products...not just for a customer relationship, but spanning a network of potentially related customers.

That holistic approach was a hot topic at the 2012 Association of Certified Fraud Examiners (ACFE) Annual Conference in Orlando, FL. In a one-hour presentation at the event, Dan Barta and David Stewart of the SAS Security Intelligence Practice described a layered approach to fraud detection, where controls are in place at multiple levels, and alerts from traditional monitoring systems are overlaid with network analysis to reveal linkages and uncover fraud that would otherwise go undetected.
Outwitting the Criminal Mind: The Challenges

Even the most well-intentioned and well-managed financial institutions face some daunting realities.

Fraudsters are more sophisticated than ever.

“When I started with the FBI 25 or 30 years ago, we didn’t even have computers – and neither did the criminals,” said Barta. Check fraud was the biggest concern of the day, and the tools to conduct it could be acquired at the office supply store.

“Now we have expanded the way people can transact business. You can deposit checks via mobile phone, and companies are paying bills via ACH, so there are a lot of new avenues involved. Every time the industry presents a new, convenient way to do business, we also present a whole new class of fraud risk.” The relative anonymity of e-commerce makes it more difficult to uncover bogus identities, man-in-the-middle attacks and hidden relationships.

Fraud has evolved from rogues to rings.

“In the old days, there wasn’t a lot of organization on the criminal side,” said Barta. “There were individuals doing check fraud, loan fraud or what have you, but now there are big organizations with multiple players and roles being played by different individuals. They’re very organized and very decentralized. People are embedded in different companies, often with players around the world. When fraud crosses international borders, it becomes just that much more difficult to chase the money.”

The velocity of fraud has increased.

“Now that fraud groups are organized, they can do a lot more,” said Barta. They can hit a city, perpetrate a lot of profitable fraud, and then they’re quickly gone. Instead of setting up a massive, one-time strike, they can do a lot of smaller activities under the radar for the same ultimate haul.

Cross-channel fraud is widespread – and difficult to detect.

From a customer perspective, banks are seen as a single brand that operates across multiple channels (ATMs, branch offices, online, call centers, mobile, etc.). From a bank’s perspective, customers are seen as diverse entities based on product – mortgage, credit card, consumer banking, small business, home equity, etc.

Criminals know this all too well. They know bank fraud systems rarely monitor customer behavior across multiple accounts, channels and systems. That vulnerability paves the way for cross-channel fraud, in which criminals gain access to customer information in one channel and then use it to commit fraud in another channel.

Credit and debit card fraud is one of the fastest-growing and best-known means of criminal profit. What makes card fraud of particular concern is that international crime rings are often involved, changing fraud from a random criminal activity into a well-organized enterprise.
Rapid transaction processing makes it easy to grab and run.

_In an accelerated banking arena, funds are collected and transferred faster than ever. That speed has helped reduce the incidence of kiting, which takes advantage of the float to make use of nonexistent funds in a bank account. On the other hand, faster processing has compressed the time available to detect fraud and mitigate risk._

Financial institutions have to watch for the enemy within.

_In a 2011 Ipsos MORI Survey, 50 corporate executives were asked which groups or activities they think are most likely to mount targeted cyberattacks against the organization. Topping the list, no surprise, was concern about organized fraud rings and professional fraudsters (58 percent). But 56 percent of respondents said they were almost as concerned about their own employees._

_With good reason. Barta talked about recent research into an organized fraud ring operating in the payments arena. “In every situation, there was an insider at the bank who was providing the information. We looked at three or four individual institutions, and the fraud in every one had an employee flavor to it. So we have to ensure that employees and internal transactions are being monitored as well.”_

Where Many Fraud Programs Fall Short

In spite of the high priority given to fraud, financial crime and security risks, traditional approaches to dealing with such risks are proving to be insufficient.

Fragmented and Reactive

In the last 25 or 30 years, the banking industry has approached fraud in a reactive manner. Every time a new problem arises, somebody builds a product or establishes a policy or procedure to address that problem. As a result, banks are operating with a patchwork of systems and tools. In the payments arena alone, a bank could easily have a dozen software systems, procedures and reports that are being worked every day.

There may be many silo initiatives just within one group. For example, in most large banks, there are multiple fraud groups: a check fraud group, an ACH fraud group, a wire fraud group, a credit card group, and so on. The industry is only now asking whether these groups should be talking to each other. Big organizations have been challenged by politics and culture, so it has been very difficult to break down the walls of the silos.

The resulting cross-channel view is critical, Barta said. “Banks are monitoring transactions and account activity but not thinking about how accounts might be related within their own portfolio of customers, let alone how fraudsters operate across multiple financial institutions. As an industry, we’re just now thinking about how to monitor and detect fraud across the entire relationship.”
“Many times, the activity in any one channel isn’t that dramatic, but when you look at the total relationship and the total activity, suddenly you start thinking, ‘Hmmmm, maybe I should start looking at this customer a little bit closer.’”

**Too Little, Too Late**

The fraud detection systems in place today typically provide reactive, after-the-fact analysis of questionable transactions – an approach that comes too late to give any real protection from loss. Few systems block transactions at point-of-service.

“The credit card business has always been very good at real-time monitoring and decision making, but very few of the other payment methods are done in real time,” said Barta. “More and more banks want to move all monitoring as close to real time as possible.”

**Ineffective Systems = Ineffective Investigations**

“The cumulative effect of all these system limitations is that investigators are not getting the full picture of a customer and the issues,” said Barta. “Because there’s no central repository for case management, an investigator in the credit card investigations department might not realize that there’s a case on that same person over in another department.”

On the alert management side, people are working the alerts and trying to determine whether there’s fraud. They are getting more and more alerts, and more and more of them ultimately don’t turn out to be fraud. On the post-fraud side, investigators are seeing more and more fraud cases that the monitoring systems have missed, so they are working more cases. It’s lose-lose.

**Layered Approach to Fraud Detection**

Where independent, product-centric, transaction monitoring systems fall short, a layered approach to fraud detection and management can be quite effective. A layered approach assesses activity at multiple levels and uses multiple analytical approaches.

“Analyst firms have weighed in on a definition of the layered approach and what it should look like,” said Stewart. “The core concept to a layered approach is that you need multiple controls, because no single control on its own is impervious to compromise or attacks. Fraudsters are going to compromise all or some of these controls pretty easily. A combination of controls provides a much stronger defense.”

Barta and Stewart discussed a five-layer model set forth by fraud analyst Avivah Litan of Gartner Group.

“Fraud detection today is largely segmented by a particular payment method. Very few banks are approaching it from a complete view of the customer relationship and the patterns the customer adopts across payment areas.”

Dan Barta
SAS Security Intelligence Practice
Layer 1: Endpoint-Centric — Secure the Points of Access

Layer 1 entails adding a band of authentication for customer access channels. The very minimum standard for low-risk scenarios is two-factor authentication, such as a combination of hardware or software ID and a personal identification number (PIN), or a user ID and password. For higher-risk scenarios, three-factor authentication is more secure but also more inconvenient. Out-of-band (OOB) authentication – which requires separate information channels for authentication and access – is widely accepted as the defense against man-in-the-middle attacks.

These controls sound fundamental, but many institutions are weak even in monitoring at this level, said Stewart. “As an investigator, one of the things I question is, ‘Does the institution do a good job in capturing failed authentications and marrying that information with other behavior?’ Not very often. It’s usually looked at in a silo.”

Layer 2: Navigation-Centric — Compare Website Behavior with What Is Expected

Layer 2 controls include real-time, dynamic capture of customer and account online activity, which is used to build a customer profile to determine what is normal or abnormal for this customer. The profile becomes a rich data store for an enhanced view of the customer/account and forms the foundation for real-time decisions. This analysis goes beyond Web analytics (hits and clicks) to understanding behavior. How does the user’s navigation behavior in the session compare to what is expected?

SAS® works with a solution from Celebrus Technologies (formerly Speed-Trap) that captures detailed, accurate, real-time data from any browser-based or online application. “It not only captures your IP geolocation, but it starts building a behavioral profile of how you behave in an online banking or online commerce session,” said Stewart. “The solution was designed to support marketing – to help understand customer shopping behavior and design more effective Web pages – but it is very applicable for understanding criminal behavior as well.”

Current Challenges for Investigators

- Monitoring and detection systems don’t keep pace with new products/offerings and schemes.
- Systems exist in product and channel silos.
- Existing systems act on a transaction or account.
- There’s little or no cross-channel view of a subject’s behavior.
- Few systems block transactions at the point of service.

---

Layer 3: Channel-Centric – Understand Users and Accounts by Channel

Layer 3 represents industry best practice at present. The concept is to have an end-to-end enterprise platform that can address a specific channel and provide extensibility across channels. For example, SAS just implemented a real-time fraud prevention system for a major US bank. The system is channel-centric for the commercial ACH and wire systems, but it views activity in the context of an account profile.

A strictly channel-centric system would detect anomalies at the account level. For instance, if an account had only two ACH transactions in the last two years, 47 ACH transactions today would be flagged as abnormal. “We go beyond that,” said Stewart. “We can look not just at what’s normal for that individual account but also what’s normal for all the accounts that roll up under a customer or commercial entity. We also identify things that are anomalous for that ACH batch for that customer.” This higher-level view provides a much better indication of what constitutes “normal” or “abnormal” behavior.

Layer 4: Cross-Product, Cross-Channel – Correlate Activity and Alerts by Entity

“We recently commissioned a research firm to conduct a study on mobile banking security, and of the 12 banks in the study – 12 of the largest banks in North America – none of them had a good key performance indicator, key risk indicator or other quantitative measure of cross-channel fraud,” said Stewart. Institutions are aware of the cross-channel threat but struggle to quantify the actual risk exposure.

At Layer 4, the institution takes a cross-channel approach to scoring transactions and entities across multiple accounts, products and channels. Transactions that initially look innocent may appear suspicious when correlated with activities in other areas. Layer 4 is pretty much the gold standard for the industry today — or at least the silver. For one client, SAS implemented a real-time fraud decision system for credit and debit card lines, and then added cross-channel detection for Asia Pacific operations. The institution is monitoring payments to credit card accounts made through phone banking, online, by check and by mobile device. Complete transaction monitoring (rather than looking at a subset of transactions) is important because fraudsters do a lot of systems testing through low-dollar or zero-dollar transaction attempts that sampling may miss.

Stewart cautioned against a solution vendor that claims to have the be-all and end-all analytic technique for your fraud program. “Some providers espouse one analytic technique or types of advanced models that they think are the best approach. We’re SAS, the market leader in analytics, so we know analytics pretty well, and we know you can’t always tell in advance which analytic technique will be most effective. When solving for unknown behaviors, we often address the problem with a hybrid approach that uses a combination of rules, anomaly triggers and models to generate alerts.”

Layer 5: Entity Link Analysis – Gain Holistic Perspective of Related Customers

Layer 5 controls go beyond transaction and customer views to analyze activities and relationships within a network of related entities (e.g., customers who share demographic data or transactions). Entity link analysis helps detect and prevent fraud by:
• Identifying patterns of behavior that only appear suspicious when viewed across related accounts or entities.

• Discovering the networks associated with an identified suspicious account, entity or individual to determine if a case is limited to an isolated individual or is part of a criminal conspiracy.

For example, the Advanced Analytics Lab at SAS created a solution that enables an automobile insurance provider to better identify fraudulent claims. The system uncovers staged accidents or false claims by identifying suspicious patterns or overlaps, such as cases where an individual is the insured party in one case and a passenger in another, or where the insured party and claimant have the same phone number, or where there is repetitive use of the same body shops and medical professionals.

The unique network visualization interface helps investigators see these connections more clearly, so they can uncover previously unknown relationships and conduct more effective, efficient investigations. In addition to detection and risk scoring, investigation teams can explore relationships that include individuals flagged by existing rules, anomaly detection or predictive modeling. Investigators have fast access to customer details and all related parties and networks, resulting in quicker case disposition.

A Closer Look at Network Analysis

Leading institutions – or at least the ones most serious about ferreting out fraud – are seeking to integrate the controls of Layers 1 through 4 and overlay those alerts with entity link analysis (also called social network analysis). Through network analysis, investigators can easily see whether customers, accounts or other entities are associated in ways that are meaningful to investigators.

Connecting the Dots

Network analysis can connect entities through demographic attributes such as address, phone number, employer, account ownership, IP address, device ID and much more.

“But just as with transaction monitoring, you have to determine whether the finding is significant, which means finding the optimum criteria to determine that two accounts are linked,” said Barta. For instance, shared employment isn’t necessarily meaningful. A financial institution could have hundreds or thousands of customers who all work for the area’s largest employers or the nearby military base. Two people could share the same address or phone numbers at different times.

That’s why a strong network analysis system also looks at transactional relationships and other behaviors. “You’re linked to me if I’m sending money to you or you’re sending money to me,” said Barta. “That’s a pretty strong link, because as a general rule, we don’t send money to people we don’t know. Where is the money moving to and from? Banks have much of this information already, and it can be a very valuable link.

“They are two classes of enterprise fraud management solutions — one detects fraudulent transactions or unauthorized activities as they occur, and one detects organized crime and collusive activities using offline entity link analysis.”

Avivah Litan
Gartner Group
“In one of the credit bust-outs we worked, the fraudsters were cultivating dozens of accounts, but all the payments for those accounts were being made from the same account at another bank. So all of a sudden, we had the means to link all those dozens of customers and credit lines to uncover an organized fraud ring.”

**Network Analysis Visual**

**Credit Card Bust-Out Example**

*Figure 2: Network analysis links entities based on demographic or behavioral attributes.*

**Bottom-Up or Top-Down?**

In using network analysis, do you start with a universe of entities and find how they are linked, or do you start with the universe of transactions, find potentially anomalous patterns that trigger alerts, and then overlay the network analysis on those specific cases?

It depends on whether you are on the detection/prevention side or the post-fraud investigation side. If you take the top-down approach (start the process with network analysis), the system will generate a fantastical constellation of connections and lots of network-level alerts, most of them inconsequential. It makes more sense to allow the Layer 1-4 monitoring systems to generate alerts and then overlay the network piece to determine if the case is an isolated incident or part of an organized fraud ring.
“In the proof-of-concept projects we have done, the top-down approach resonated much more with the post-fraud investigator who was putting a case together,” said Barta. “Starting with a referral from the fraud detection and prevention group or customer-reported incident, they could start the network analysis with the customer in question and see where the network connections lead them. In several cases, the fraud exposure was significantly larger than anticipated. And as we know, the bigger the case you can put together, the more likely it is to be investigated by law enforcement and prosecuted.”

Anatomy of a Credit Card Bust-Out

Over an 18-month period, seven separate customers open credit card accounts with the bank, some with credit limits of $2000 or so, others up to $20,000. Each customer engages in very normal account activity. They use the cards at merchants to a normal degree. They make the customary and usual payments – for a while.

Customer 1 continues as usual, but in two months’ time, Customer 2 makes three $6500 payments in the same day at multiple branches, even though his credit limit is only $3000. Then he turns around and gets an ATM cash advance. Curious behavior. A few days later, the same thing.

Those $6500 payments come back dishonored by the drawing bank, but by that time the customer has run up the card to its limit – twice.

Customers 3 and 4 exhibit a very similar pattern. Then Customers 5 and 6 come on the scene but do nothing notable. Customer 7 shows suspicious account activity, and the bank closes the account.

On a simple transaction monitoring level, five of the seven accounts would have been flagged. Even Layer 3 controls would have picked up the signals: payments exceeding the balances or the credit limit, multiple payments in the same day at different branches, and large multiple cash advances. But social network analysis immediately revealed something even more interesting.

“All seven of these customers had the same employer phone number – a granite and tile company that had no website and no storefront,” said Barta. “Without even looking at corporate records, credit reports or talking to other tenants at the address, we could see that this was a fictitious company – and determine that accounts for Customers 5 and 6 were being cultivated to bust out as well.”

Looking at the timeline, now that we know these customers are linked, would the bank have acted differently? Of course it would. With two of the first five related accounts already closed, the bank would have managed the other customers much more cautiously, if it opened the accounts at all. There’s a lot to be learned by looking at the entire picture, far beyond credit reports and the data on the application.
Enterprise Fraud Management in Action in Other Industries

The SAS Advanced Analytics Lab, a center of excellence for complex analytical projects, started working on practical applications for entity link analysis about four or five years ago. Stewart shared examples from other industries.

Curbing Abuse of Government Assistance Programs

The Department of Social Services of a large US county was experiencing fraud, waste and abuse in public assistance programs. The county engaged SAS to determine if data analytics and visualization could help detect opportunistic and organized fraud in its childcare program.

SAS analyzed six years of historical data from five different source systems (claims, payments, application, third-party and fraud case data). “What we found was astounding,” said Stewart. “The estimated save was $31 million annually in improper benefits and a $3 million savings in investigator efficiency. The system had an 83 percent hit rate detecting daycare providers engaging in fraud and a 40 percent hit rate identifying fraud among participants.”

“Investigating fraud, waste and abuse in government programs can be a lot like finding money on the ground. The potential gains and savings are enormous.”

David Stewart
SAS Security Intelligence Practice
In most instances, the recipients were in collusion with the providers to receive the benefits, connections that would be immediately obvious with network visualization. In addition, a terrain map overlay showed that some people were allegedly driving 45 to 50 miles a day through the mountains to take their children to daycare. A satellite map overlay showed some daycare centers were located at vacant real estate properties. “So this pilot program was wildly successful,” said Stewart, “enabling the county to identify 32 times more fraud rings annually at less cost.”

**Detecting Underreporting or Abuse of Workers’ Compensation**

SAS worked with a state labor department that provides workers’ compensation for more than 2.5 million workers employed by 171,000 employers. The department collects premiums and pays out more than $1.4 billion a year, making it the eighth-largest workers’ compensation insurance company in the country. Abuse of the system occurs when employers underreport hours, report hours in an improper risk classification with lower premium rates, or don’t register or pay at all.

“In 2009, the department estimated it was losing about $100 million annually,” said Stewart. SAS analyzed data from 30 disparate source systems to detect misuse of the system, especially employers that are not registered and not paying into the system or those drawing too much out.

“The results of this project were so good that the IDC analytics group did a 25-page case study on it,” said Stewart. “This project came in $3 million under budget and provided a two-year payback, which rarely happens in a government project with technology firms.” The department conservatively estimates a savings of $11 million to $14 million of recovered premiums in the first year – a 57 percent lift over legacy processes.

A similar pilot project in another state identified nearly $12 million in evaded workers’ compensation premiums and recovered $1.2 million. Based on this success, SAS software will be rolled out to all agencies as the state becomes the first to institute a statewide approach to fighting fraud.

“*We saw a lot of anomalies, where someone would claim employees at a very high-priced risk level – and then after a claim, a temporal analysis in subsequent months showed that they didn’t have any employees that fit into that high-risk category.*”

David Stewart
SAS Security Intelligence Practice
Closing Thoughts

The financial services industry needs more than traditional fraud detection and investigation methods based on silo monitoring systems. The growing sophistication, complexity, velocity and impact of cyberattacks require a more robust approach with controls at multiple layers:

- **Layer 1: Endpoint-centric** – At the point of access authorization.
- **Layer 2: Navigation-centric** – In behavioral analysis of website navigation.
- **Layer 3: Channel-centric** – At the aggregated customer level by channel.
- **Layer 4: Cross-channel, cross-product** – Across channels and bank products for an entity.
- **Layer 5: Entity linking** – Understanding connections among related entities.

Most financial services institutions have implemented some form of controls at Layers 1-3. Those that achieve Layers 4 and 5 can be said to have adopted the enterprise fraud management approach that SAS supports and endorses. The criminal masterminds deserve nothing less.
About SAS

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS helps customers at more than 60,000 sites improve performance and deliver value by making better decisions faster. Since 1976, SAS has been giving customers around the world THE POWER TO KNOW®. For more information on SAS® Business Analytics software and services, visit sas.com.