White Paper

Find the digital fingerprints of fraud in the financial services industry

Velocity and pattern detection tool adds powerful capabilities for next-generation fraud management

Gasan Awad
Vice President, Fraud and Identity Product Management

Andrew Smith
Senior Vice President, Fraud Analytics

May 2012
Find the digital fingerprints of fraud

Velocity and pattern detection tool adds powerful capabilities for next-generation fraud management.

Fraud management, risk management and marketing teams need all the help they can get in the fight against fraud. With limited budgets, they’re expected to keep pace with the latest fraud trends and protect against weaknesses in their organization’s fraud defenses.

Applying pattern detection technology to your own data is a good start—but it doesn’t detect suspicious activity that’s occurring outside your organization.

This paper discusses the current challenges of fraud control in the financial services industry, especially at account open, and introduces a new, velocity-based fraud solution from Equifax.

Challenges in fraud management

Financial services organizations deal with consumers and valuable assets so they must also deal with fraud. Armed with identity information acquired through data compromise, hacking, social engineering, or social networking, fraudsters are constantly on the lookout for vulnerabilities to attack those valuable assets and fraudulently open new accounts.

Most financial services organizations have a number of fraud prevention measures already in place to curtail losses from fraudulent applications. These measures typically include an account open fraud screening solution on the front-end and additional measures for high-risk transactions once the account has been opened. Depending on the type of tool, the effectiveness can vary greatly but most financial services organizations have a minimum of two defenses already in place.

For every advance in an organization’s fraud protection tools, fraud groups soon discover what’s in place and start searching for ways to circumvent that defense. Mercator Advisory Group calls this “the balloon effect,” where fraudsters constantly probe for the most vulnerable and least defended areas and focus their efforts there. It is very important for a financial services organization to deploy current defenses and to be perceived as a “hard target” for fraudsters so they will steer their primary efforts elsewhere.

However, the fight against fraud does not occur in a vacuum. Many fraud managers will tell you that it’s easy to stop 100% of the fraud impacting their organization; just stop 100% of the applications and transactions entering their organization. Obviously, this is not a realistic outcome, especially because the most profitable avenues for acquiring new business—mobile and online—are the most vulnerable to fraud. What a fraud managers needs are tools to stop fraud without substantially interfering with the flow of “good” applications and transactions. It’s a balancing act, and one for which fraud managers are always looking for new solutions.

Mobile and social media trends add to fraud risks

Users of Facebook, Twitter, LinkedIn and other social media tend to share significant amounts of personal information that their financial services providers commonly use to authenticate identities. According to Javelin Strategy and Research’s 2012 report on identity fraud, Javelin found that:

- 68 percent of people with public social media shared their birthday information,
- 18 percent shared their phone number, and
- 12 percent shared pet names
Velocity is the frequency that data attributes or relationships occur over a period of time. Unusual spikes in frequency in various data elements or attributes can indicate suspicious patterns of activity.

Fighting fraud with fewer resources

Fraud management, risk management, and marketing teams are expected to contain fraud costs with budgets that don’t necessarily keep pace with business growth and new fraud trends. Consequently, fraud teams must employ better defenses to maintain or improve fraud capture rates against existing and emerging fraud threats. And, they must do this without creating excessive manual review volumes that increase overhead costs, limit the organization’s ability to scale and accommodate workflow fluctuations, and present their own accuracy issues.

Fraud teams need help—they need tools that are current, dynamic, efficient, and effective in finding patterns that point to fraud. Traditional identity fraud screens alone can’t keep up with all the techniques used for identity theft, synthetic identity creation first party fraud, and other major fraud schemes.

Internally focused fraud prevention tools and strategies are important components of a multi-layered approach to fraud, but they are not enough to prevent fraud from the most advanced criminal groups. For example, conventional screening tools often don’t uncover suspicious relationships between components of an identity or rapid spikes in activity on a specific identity component such as the address, phone number, or Social Security number in a short period of time. In addition, conventional fraud screening tools do not see an identity’s activities across the entire network of financial services organizations and other relevant industries.
“Waterfall” screening with fraud management tools

We know fraudsters are well financed, organized, and technologically sophisticated. They troll target websites, submit test applications, and often gain insider knowledge looking for the weakest links in account opening processes. Real-time fraud detection measures are essential for financial services organizations to keep pace with the fraudsters while ensuring that the good applications can get through timely.

A typical fraud protection waterfall

Most fraud defense mechanisms have evolved from a single defense technique to a multi-layered, waterfall strategy. The earlier in the waterfall that a decision about a consumer can be made the better since each step tends to add incremental expense for the institution and incremental friction for the consumer. This can and often does result in lost or delayed revenue.

A typical multi-layered approach might be:

1. Ensure that identity components actually exist
2. Compare components against internal and external “hot lists”
3. Run the applications through a basic fraud heuristic
4. Present knowledge-based authentication questions to higher risk applicants
5. Perform manual reviews on the applicants that can’t successfully complete authentication questions

According to researchers, fraud managers spend 52% of their budget on manual reviews which limits their investments in new technology and human capital. This places a premium on an organization’s passive fraud checks, executed early in the waterfall process without the interactive participation of the consumer, so that good applicants can be pulled through quickly. Because passive fraud checks are invisible to the consumer, they are generally preferred over active checks. After all, customer communication channels should be filled with marketing messages, not fraud messages.

Active v. Passive fraud checks

Active checks require the applicant to be involved in the process. They may be required to:

- Answer interactive questions
- Mail in additional documentation
- Provide out-of-band authentication

Some customers struggle to answer questions and asking customers to mail in additional items always creates some level of fallout.

Passive checks operate in the background and are transparent to consumers. These checks can include:

- Social Security number verifications
- Validating applicant-supplied information against outside sources
- Other risk-based assessments of an identity’s likelihood of fraud. This keying technology consolidates records from hundreds of millions of consumers by assigning unique identifiers or “keys” to every consumer to help discern their true identity despite subtle variations in the data.

Passive defenses early in the process pull through the good applications quickly with minimum operational expense and revenue loss. This results in the maximum return on marketing dollars and happier customers.
Network pattern detection plays a vital role in next-generation fraud management

Technology for velocity and pattern detection is a powerful weapon in the fraud management arsenal. Simply put, velocity is the frequency that data attributes or relationships occur over a period of time. And, unusual spikes in frequency for various data elements or attributes can indicate suspicious patterns of activity. These anomalous applications are then flagged and scored for fraud risk and sent for further investigation.

Financial services organizations are no stranger to the concept of data analytics and behavioral patterns to detect fraud. After all, many have been doing exactly that with their internal data and transaction monitoring systems for years. For most organizations, though, the ability to spot fraud patterns is limited to what they can detect within their walls.

Fraud experts agree that detecting patterns with internal data alone is not sufficient. “In play” identities may be active in other financial services organizations, and these patterns need to be detected before the compromised identities spread.

External velocity and behavioral pattern tools are critical to spot personally identifiable information that may be in play with fraudsters. In cases of synthetic identity fraud, for example, the tools provide an earlier warning of an identity with an anomalous volume of applications and inquiries. Tools like this can help prevent the kind of movement across victim organizations that fraudsters typically do to avoid detection.

External velocity and behavioral pattern detection tools are already in the market, but many suffer from at least one of the following weaknesses:

1. **Insufficient volume of data.** To realize the full promise of pattern recognition, massive data resources are critical. Few data providers have assets available to achieve the high capture rates demanded in this competitive marketplace.

2. **Stale data.** Fraudsters move quickly because their assets, stolen identities for example, tend to degrade in value rapidly. Suspicious activity must be detected in a few hours or days of the occurrence, not weeks or months after the activity begins.

3. **Cumbersome tools for data analytics.** Financial services organizations often do not have ready access to the data and tools they need to make sense of their information.

The result is a:

- Limited number of attributes to work with;
- High number of false positives; and
- Narrow view of the application universe.

---

Equifax fraud management experts offer the following suggestions:

1. **Focus significant prevention measures on the first line of defense:** account opening processes. Use a multi-layered approach to detect fraud at account opening and monitor volumes closely. Combining alerts can be essential for real-time, multi-channel defenses to address a wide spectrum of fraud threats. (Download the Equifax white paper, Account Opening: The Front Door of Fraud.)

2. **Use internal data and analytics to detect hidden patterns for new applications and within existing accounts.** Tip-offs to fraud from internal analytics might include application anomalies, unusually high purchases of popular items, or multiple accounts being opened in a short period of time with data in common.

3. **Use external consortium data with velocity and pattern detection to be alerted to suspicious behavior by that applicant at other organizations.** Schemes that are in progress elsewhere may not hit your organization right away. However, if you’re only analyzing your own data for behavioral fraud patterns, it may be too late to stop the fraudsters from gaining a foothold. With velocity and pattern detection alerts, your organization will detect suspicious activity that would have otherwise been missed.
Suspicious ID®—the new Equifax solution for velocity and behavioral pattern detection

A powerful new solution is now available from Equifax to help detect hidden patterns of application behaviors that may be indicative of suspicious and fraudulent activity.

With access to millions of daily inquiries, Equifax is uniquely positioned to apply analytics, velocity detection and behavioral pattern detection to the problem of managing fraud losses with minimal damage to legitimate customers. Leveraging our proprietary keying and matching technology, the new solution spots important anomalies in application and inquiry activity. Based on your rules, a suspicious application will be isolated and queued for additional review. Just as importantly, a greater population of legitimate applications can be passed through rapidly without the need for additional review, expense, and applicant fallout.

What differentiates Suspicious ID from other pattern-detection services in the marketplace?

- **Extensive data:** Suspicious ID is connected to the richest source of identifying information supplied by thousands of institutions from relevant industries. Members supply reports to Equifax daily from more institutions and industries than any competitive service. Suspicious ID captures and analyzes billions of identity data elements across thousands of institutions.

- **Speed and timeliness:** The data assets behind Suspicious ID are continuously refreshed with confirmed fraud reports, proprietary alerts, and millions of daily inquiries. The Suspicious ID network collects identifiers in real-time as information streams from consortium members and other unique data sources. Just as importantly, a greater population of legitimate applications can be passed through rapidly without the need for additional review, expense, and applicant fallout.
- Fewer false positives: As part of the Suspicious ID solution, Equifax uses proprietary keying technology to manage and link consumer information. This keying technology consolidates records from hundreds of millions of consumers by assigning unique identifiers or “keys” to every consumer to help discern their true identity despite subtle variations in the data. This ability to link names, addresses, and phone numbers to a single identity or household is important because it significantly reduces the chance that consumers with information in common will be mixed up or confused. The result is fewer false positives so you can decrease the number of expensive manual reviews required and a better fraud hit rate.

Suspicious ID delivers over 80 unique attributes that can be leveraged to provide deep insights into suspicious application and fraud patterns across industries. It also delivers a sophisticated scoring model to better assess cut-offs for application risk segmentation.

The Suspicious ID score provides an effective way to segment applications—maximize capture rates and minimize false positives into the smallest possible segments to escalate detection and treatment.

Suspicious ID can be bundled with eIDVerifier, and other Equifax fraud mitigation products, to create an integrated fraud waterfall strategy to help fight true-name fraud, synthetic fraud, first party fraud and other significant fraud threats.

Pattern detection with Suspicious ID: real-world results

The value of Suspicious ID has been validated by a number of different institutions including:

- Credit card portfolio at a leading global bank
- Demand deposit accounts at a major financial institution
- Telecommunications products at a top telecommunications carrier
Credit Cards

In recent years, the credit card industry has been heavily focused on instant credit applications and online channels to drive growth while containing operating expenses. In this case, the bank that piloted the Suspicious ID solution was looking to reduce fraud charge-offs and operating expenses without negatively impacting the customer experience. Equifax performed the analysis on historical fraud data and showed the bank they could improve the fraud capture rate and decrease manual reviews using our patented fraud pattern and velocity detection solution.

The bank's existing fraud rate was contained at 0.5% but the average loss per incident was fairly substantial. The Equifax analysis showed that the Suspicious ID solution was able to capture 11.5% of fraud that was not captured by their existing defenses at a false positive rate of 30:1. Based on industry averages and by including Suspicious ID in their account opening processes, the bank is on track to save to $1.2 million dollars a year.

Demand Deposit Accounts

In recent years, the banking industry has seen a substantial increase in deposit account fraud. This is a logical progression for some of the more elaborate fraud types because a deposit account is one of the vehicles used to facilitate fraud on other accounts. In addition, worthless deposits can be very lucrative to fraudsters and costly to financial services organizations.

In this case, the existing false positive rate for the bank was 53:1. The Equifax Suspicious ID solution was used to isolate the most important attributes. The result was a reduction in the false positive rate from 53:1 to 15:1 or a 72% improvement and the projected savings for that bank is $500,000 each year. In both lines of business (DDA and Cards), the lift was significant from using the velocity and behavioral pattern attributes. Based on industry averages and by including Suspicious ID in their account opening processes, the bank is on track to save $700,000 dollars a year.
**Telecommunications**

In recent years, devices offered in the telecommunications industry have become increasingly valuable and a higher target for the organized fraud groups. Smartphones, digital video recorders and satellite dishes are a few of these highly coveted devices. The telecommunications company looked to Equifax for solutions that would help reduce both fraud charge-offs and manual review expenses, without negatively impacting the customer experience.

The analysis showed that Suspicious ID could not only capture significant fraud applications, but could do it a low false positive rate. Equifax identified 11 attributes that were each able to capture over 1% of fraud at a false positive rate of less than 30:1. Based on industry averages and by including Suspicious ID in their application opening processes, the telecommunications company is on track to save $1.9 million dollars a year.

“The next generation of enterprise fraud management solutions offers a unique combination of real-time alerts and behavioral analytics across multiple channels, giving you complete visibility into activity on the corporate network and from other sources.”

— Bank Info Security
Conclusion

When financial services organizations use external data sources to their maximum capacity, it will provide vital fraud alerts that you otherwise would not have access to, especially in vulnerable account opening processes. With a newly available velocity and behavioral pattern detection tool from Equifax, fraud managers can apply new and powerful layers of fraud prevention before ever having to get the consumer involved.

To detect suspicious applicants at other organizations, it is essential to use robust solutions that achieve high-capture rates by interpreting massive volumes of data in real-time.

When contemplating something new to complement your existing suite, be sure to look for a solution that offers:

- Comprehensive data coverage from thousands of consortium members supplying millions of records daily
- The ability to add meaningful context to vast amounts of data through sophisticated record-keying technology, analytics, scoring and attribute reporting
- The ability to deliver scores and attributes based on real-time data, reported timely by consortium members

References


² Meyers, Christine. “Detecting and Deterring ACH and Wire Transfer Fraud”


Contact Us Today

For more information, please contact:
www.equifaxfraudsolutions.com
888-213-5301.
www.equifax.com