ORACLE
FINANCIAL SERVICES

Prevention:

Closing In On the Final Mile of Fraud Management

ORACLE WHITE PAPER | APRIL 2017

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

.

Introduction

There is no shortage of ingenuity when it comes to financial crime and fraud. We see this daily as fraudsters continuously adapt their approach and methods in an effort to stay one step ahead of the law and the latest detection technologies.

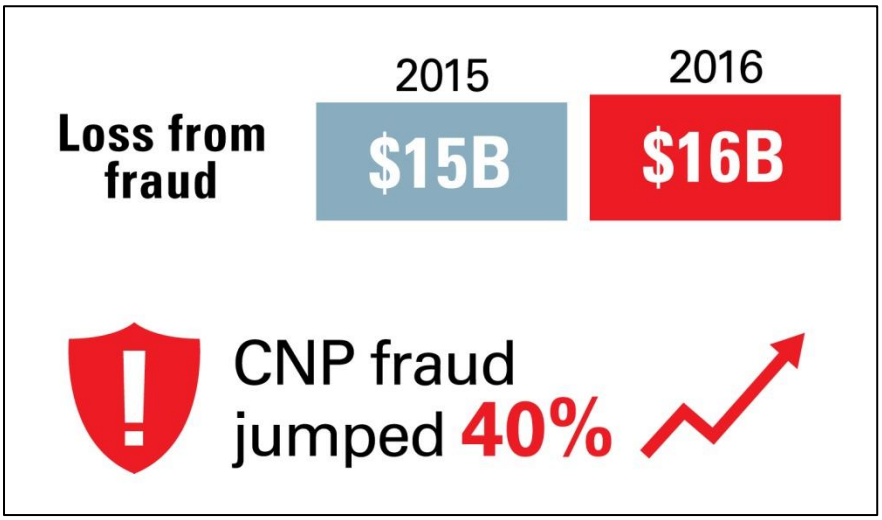
As transactions become increasingly digital and the internet of things (IoT) matures, the opportunities and avenues for fraud multiply exponentially; so do the challenges for financial services organizations.

The velocity, complexity, and expanded opportunity for financial crime require financial services organizations to rethink and retool their approach to fraud management. Real-time and enterprise-wide define the gold standard toward which today's firms aspire. Only with these capabilities can financial services organizations close in on the final mile of fraud management: prevention.

Constantly Evolving Threat

Fraudsters continue to demonstrate unbridled creativity and determination in their criminal pursuits. In turn, financial institutions must be equally diligent and agile. Criminals appear to have the upper hand right now as fraud spiked to new highs in 2016.

A January 2017 report from Javelin Strategy and Research, "2017 Identity Fraud: Securing the Connected Life,[1]" pegs loss from fraud at $16 billion in 2016, up nearly a billion dollars from the year before. Notably, card-not- present (CNP) fraud jumped 40%—criminals are moving online as chip-based cards become the norm in North America.



Source: Javelin Strategy and Research, 2017 Identity Fraud: Securing the Connected Life

The rise in CNP crime is likely to continue to soar as fraudsters use botnets and other technologies that accelerate criminal acts and reduce the risk of getting caught. New account fraud also continues to gain momentum as criminals buy stolen information and use it to set up a new account. This type of fraud can go undetected for longer periods of time as the victims are often unaware as they are not seeing any abnormalities on their statements. According to Javelin, account takeover (ATO)—in which thieves use stolen information to access an account and have a new card sent to them—spiked unexpectedly last year, up 61% from the year before and accounting for more than $2.3 billion in losses.

Mobile accounts are also under siege as transactions grow in this channel. The number of breached phone accounts doubled in 2016, with thieves intercepting e-mail and text messages related to one-time password alerts, and then leveraging that data to commit fraud. In addition, according to a 2016 fraud cost report from risk solution provider LexisNexis[2], successful fraud transactions perpetrated via the mobile channel using debit cards grew to 40% in 2016, compared to 24% in 2015.

And the beat goes on. With every payment innovation, including the rise of person-to-person payment systems, we can and must expect that threats and criminal creativity will evolve in lockstep.

[1] 2017 Identity Fraud: Securing the Connected Life. Javelin Strategy and Research, January 2017. https://www.javelinstrategy.com/coverage-area/2017-identity-fraud.
[2] 2016 LexisNexis True Cost of Fraud Report. LexisNexis, May 2016. https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2016.pdf.

New Reality, New Requirements

In this increasingly complex environment, financial firms have begun to embrace a risked-based approach to managing fraud detection. That's not to say, however, that they have perfected this model. Many financial firms rely on inflexible, disparate rules-based risk and compliance point solutions that detect specific anomalies within large data sets.

This point-solution strategy does not yield the enterprise-wide view of customer activities across channels and products required to effectively identify all threats. More importantly, it does not provide real-time detection capabilities. Organizations, therefore, are left to identify and investigate fraud well after it happens, as opposed to while it is happening, which would allow them to stop incidents immediately and, ultimately, prevent future attacks.

Further, many legacy systems do not provide the flexibility needed to quickly and effectively meet changing regulatory requirements. Instead, they require customizations that are expensive and time consuming to build and maintain, and they still do not yield enterprise-wide visibility.

In recent years, firms have gotten better at monitoring fraud across channels and achieving real-time visibility. This still is not good enough, however, as we've seen fraud continue to proliferate and the direct and indirect costs of "managing" it spiral. In this environment firms must not only focus on making their fraud-detection environments stronger, but smarter and more efficient, too.

As fraud detection methods have evolved, an unwelcome side effect has been a growing number of false positives. Many leisure and business travelers have experienced the frustration of having their credit cards denied due to suspicion of fraud when away from home on travel. As individuals become increasingly mobile, they expect their banks to keep up with them as they transact, wherever that might be, and without added inconvenience. False positives are very frustrating for consumers and expensive for firms to investigate. As important, they erode the customer experience—a critical factor in customer retention.

In this environment, financial institutions are looking to achieve real-time, enterprise-wide fraud management that goes well beyond detection and closes in on the ultimate goal: prevention. This holistic approach enables firms to more effectively identify precipitating events leading up to fraud and automatically place a hold before approving a transaction or transferring funds—while reducing the incidence of false positives.

Increasingly, machine learning is beginning to factor into the need for both stronger and smarter fraud detection and prevention environments. With billions of transactions daily and fraud transforming at breakneck pace, organizations and firms are looking to automated learning to rapidly identify anomalies and recommend action with regard to the validity of a transaction. It is increasingly the cornerstone for more effective and cost-efficient detection and prevention.

Enterprise Grade

Oracle Financial Services Enterprise Fraud Management is designed to meet the rigorous requirements of today's financial services organizations. It delivers seven unique capabilities that enable firms to go beyond reactive fraud detection into the coveted realm of fraud prevention. The integrated solution, which is part of the Oracle Financial Services Analytical Applications suite, features:

- **A standard data model across all customers** that includes pre-packaged routines to load and pre-process data from source systems. The data model stores customer, account, and transaction data as well as a rich set of behavioral data, such as ATM withdrawals, purchases, and international wires done on daily, weekly, and monthly basis, to support complete visibility across the banking ecosystem.
- **Sophisticated behavior detection powered by machine learning** (see figure 1) that identifies complex behaviors and patterns that evolve over time and are indicative of more sophisticated, complex fraud activity, such as bust out fraud. In these cases, a fraudster (who might have stolen the identities of hundreds or thousands of individuals) will apply for credit from lenders using similar last names. The fraudsters make good payments on time and ask to increase their credit line over a period of six to 18 months, looking to optimize how much money they can get from the bank before they "bust out" and go delinquent. To identify such complex patterns over lengths of time, Oracle's solution uses advanced machine learning, including sequence matching and network analysis. Machine learning is vital to more effective and cost-efficient fraud protection and prevention strategies and is replacing more cumbersome and less accurate rules-based risk-management approaches.

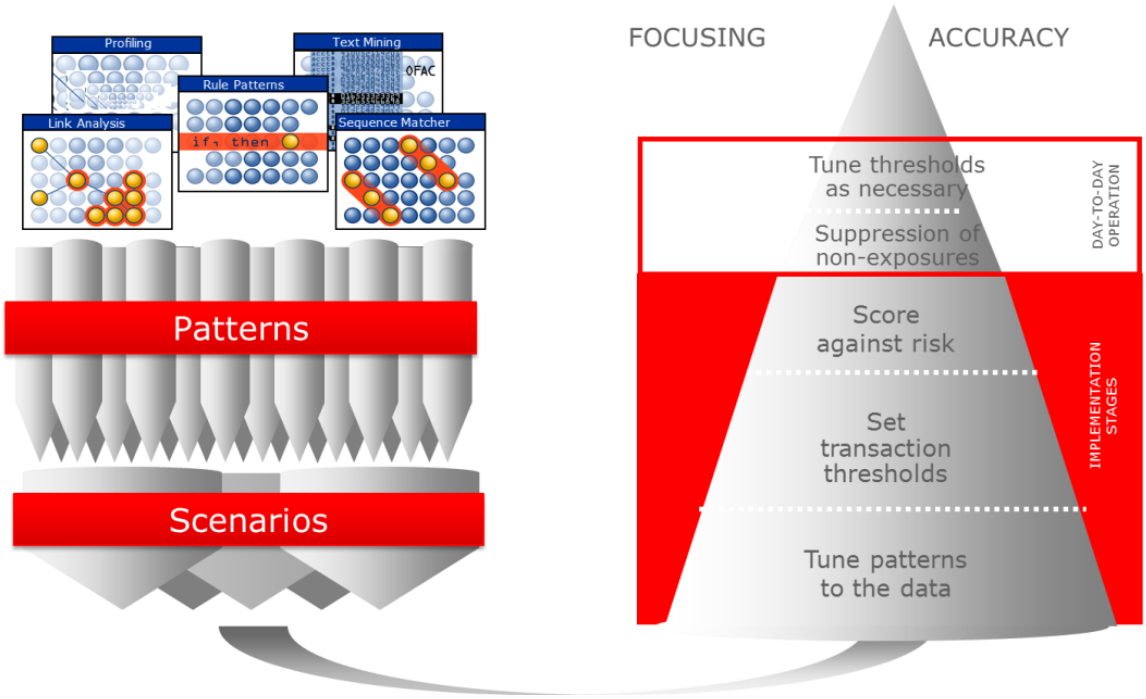


Figure 1. Behavior Detection

» **Comprehensive decision support** thanks to an inline processing engine that can evaluate and assess scores on incoming transactions in real-time, near real-time, or batch to enable immediate decisions about holding or approving transactions. The solution provides a comprehensive set of fraud scenarios, sophisticated behavior detection and profiling techniques, and advanced risk scoring that drives more targeted and effective fraud detection for current and future schemes (see figures 2). For example, batch scenarios enable firms to see long-term patterns and compare them to current scenarios. With this capability, a bank can identify, for instance, whether a customer's shopping patterns may have changed suddenly. In addition, real-time scenarios enable financial institutions to identify unlikely travel patterns or flag that a "customer" has tried to access multiple ATMs in rapid succession or entered incorrect pin credentials three times in a row.

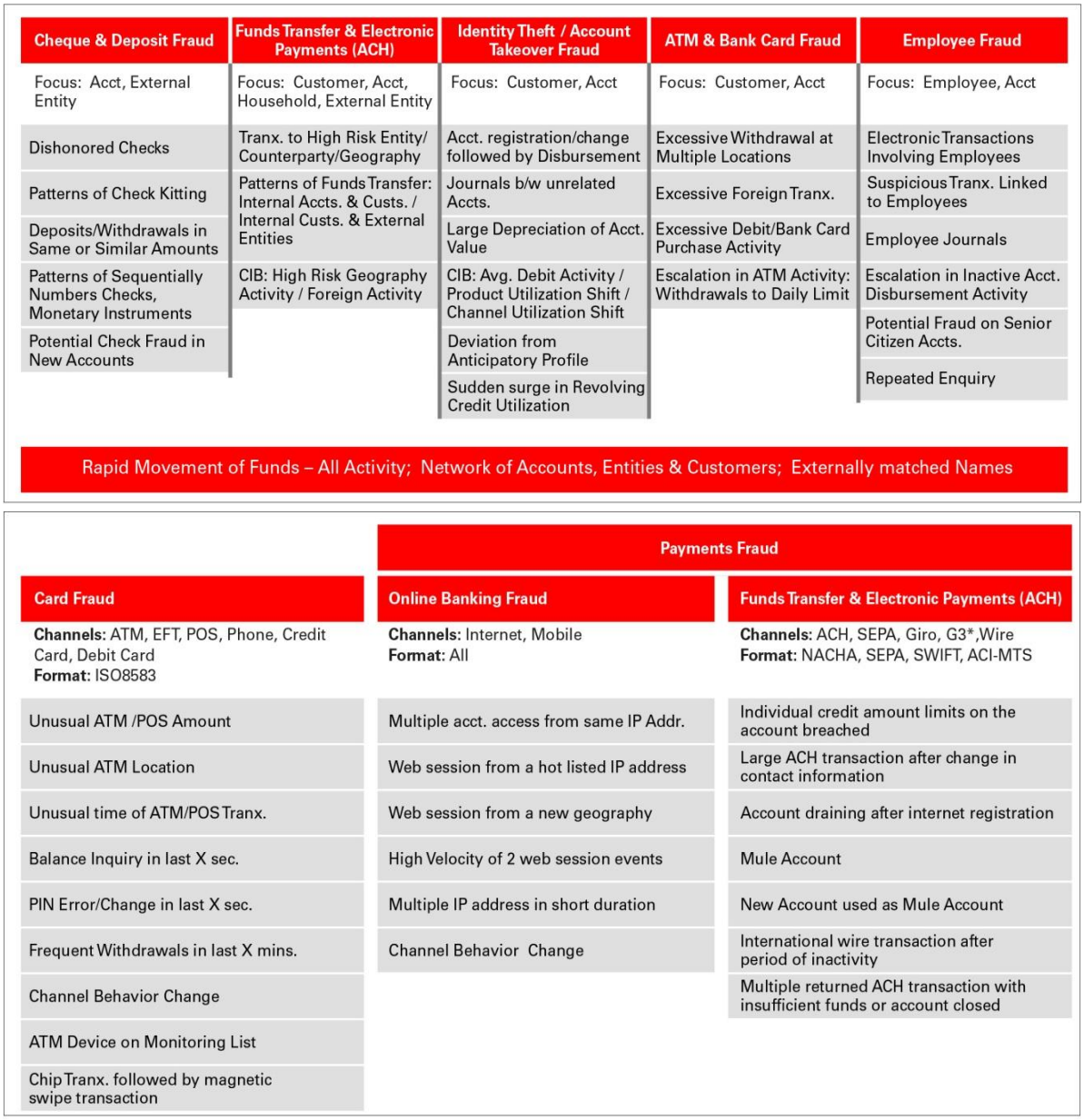


Figure 2. Scenario Library (Fraud Type)

» **Advanced analytics based on Oracle R Enterprise**, which provide a library of modeling techniques that can be invoked from an inline processing engine to help institutions more rapidly identify evolving fraud patterns. The predictive engine will apply algorithms to future events, improving the bank's ability to flag and halt fraud.

» **A single, proven platform that enables an enterprise to detect all types of financial crime** (see figure 3), such as wire fraud, ACH fraud, phishing schemes, money laundering, and more from a single solution. Oracle Financial Services Enterprise Fraud Management includes a configurable framework for data integration, workflows, integration of third-party systems, and loss capture to support this goal. The solution enables line-of-business managers to get alerts from both internal and external systems, such as FraudNet, Early Warning System (EWS), Falcon, and CHEXSystems, which is a key requirement for an enterprise-wide view of risks and potential threats.

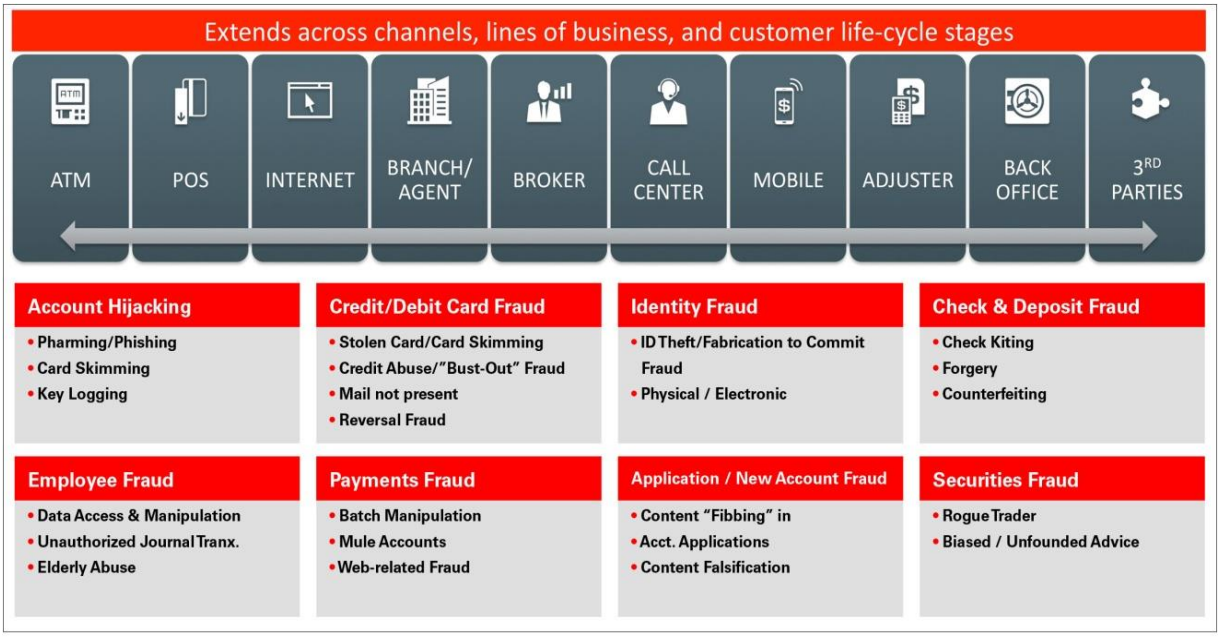


Figure 3. Enterprise Fraud Management Functional Coverage

» **Enterprise case management to optimize effectiveness and drive operational benefits and business process improvement.** The primary reason for the low return on investment for fraud management environments is the lack of information integration across existing third-party systems—requiring firms to track significant data outside the investigation process. This reduces the effectiveness of the case management tool, making it a mere repository of investigations. Furthermore, decisions made or actions taken inside a case management solution are often of importance within the original, external source systems; therefore, an information feedback loop from case management back to these systems is also critical. Oracle Financial Services Enterprise Case Management allows financial institutions to actively manage risk with a 360-degree view of all financial crime investigation data. While investigating a case, analysts have a single view of other compliance alerts, assessments and cases involving the same or related entities. Financial institutions can easily maintain and share individual alerts and cases across all financial crime and compliance systems with standardized information exchange formats. In addition, analysts and investigators can make quicker decisions by analyzing integrated data and intelligence and can automatically exchange and share information with other lines of business, law enforcements agencies, and regulators. Further business users gain context from investigations across all channels through intelligent, automatic, and configurable correlation and prioritization. Network visualization further supplements this capability by identifying hidden, high-interest network patterns across multiple channels and business lines.

» **Strong analytics for anti-money laundering and fraud along with compliance risk reporting through dashboards and powerful ad-hoc reporting** thanks to Oracle Business Intelligence**.** These capabilities put insight into the hands of senior management, empowering them to execute risk-based fraud management. For example, they can see that the firm has a credit portfolio of $10 billion and total losses from fraud of $2 million annually. From there, they can make informed decisions about whether to allocate more resources to fraud detection and management in this area or whether it is manageable at the current level—with additional investment offsetting gains. As important, the solution supports broader governance risk and compliance (GRC) initiatives, including standardization of reporting practices and methodology across channels and the enterprise.

Conclusion

Historically, financial institutions have been forced to assume a largely reactive stance with regard to fraud management—addressing one type of fraud in a specific channel only to have another threat emerge elsewhere in the enterprise in its wake. Firms have traditionally had to rely on a series of point solutions that could not deliver the end-to-end view and immediate insight required to effectively mitigate and, ultimately, prevent increasingly sophisticated financial crimes. Oracle Financial Services Enterprise Fraud Management is changing the game with a powerful integrated solution that enables an enterprise-wide approach to fraud management combined with real-time decision support—powered by machine learning—that equips firms to stop even the most creative fraudsters in their tracks.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/financialservices
facebook.com/oraclefs
twitter.com/oraclefs
oracle.com/financialservices

Integrated Cloud Applications & Platform Services

Prevention: Closing In On the Final Mile of Fraud Management
April 2017