

A Practical Guide to Anomaly Detection

Implications of meeting new FFIEC minimum expectations for layered security





A Practical Guide to Anomaly Detection: Implications of meeting new FFIEC minimum expectations for layered security

Table of Contents

INTRODUCTION	1
MINIMUM LAYERED SECURITY EXPECTATION – ANOMALY DETECTION.....	1
ONLINE BANKING FRAUD PRIMER: YOUR INSTITUTION AND YOUR ACCOUNT HOLDERS ARE UNDER ATTACK	2
INSTITUTIONS ARE UP AGAINST WELL-FUNDED, ORGANIZED CYBER CRIMINALS	2
INSTITUTIONS MUST PROTECT THEMSELVES FROM A WIDE ARRAY OF THREATS.....	2
WHY ANOMALY DETECTION IS A POWERFUL FOUNDATION FOR LAYERED SECURITY	3
DETECTING SUSPICIOUS ACTIVITY: ANOMALY DETECTION BASICS	4
HOW ANOMALY DETECTION FIGHTS CURRENT AND FUTURE THREATS	7
THE PRACTICAL OPERATIONAL AND TECHNICAL IMPLICATIONS OF DEPLOYING ANOMALY DETECTION	8
RESPONDING TO SUSPICIOUS ACTIVITY	9
ROI OF ANOMALY DETECTION	10
SUMMARY	11
ABOUT GUARDIAN ANALYTICS	11



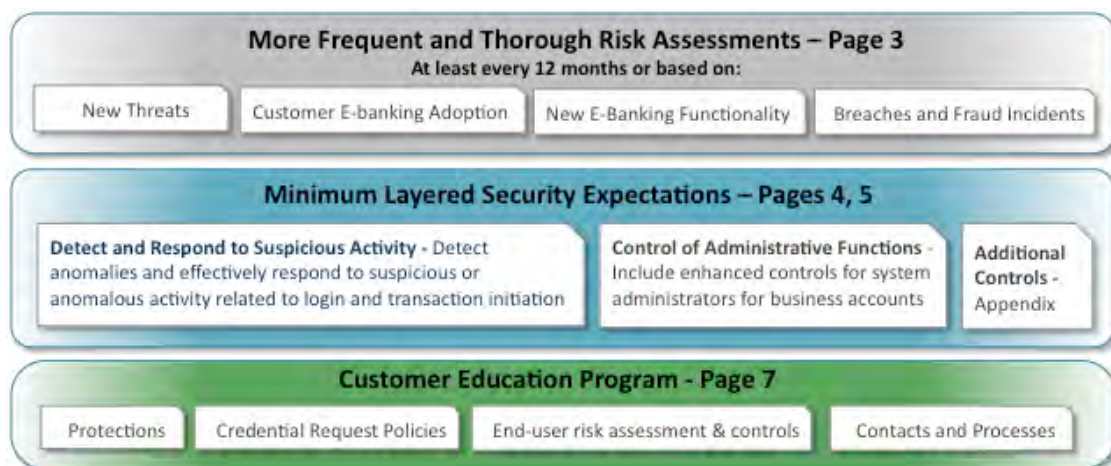
INTRODUCTION

Commercial and retail account holders at financial institutions of all sizes are under attack by sophisticated, organized, well-funded cyber criminals. These attacks have resulted in billions of dollars lost and damaged relationships between financial institutions and their account holders.

The risks are so high that the FFIEC was compelled to update its 2005 *Authentication in an Internet Banking Environment* guidance. The June 2011 Supplement clearly articulates that authentication alone cannot address today's threats and institutions must do more to protect themselves and their customers. The guidance also references approaches such as simple challenge questions and simple device identification are no longer acceptable as primary controls.

The Supplement provides new levels of clarity and raises the bar for institutions across three major areas:

- **Risk assessments** – The Agencies expect that institutions will perform risk assessments every 12 months or as the internal and external environment changes. Institutions are expected to immediately perform their assessment, create a gap analysis, establish a plan to fill the gaps, and begin executing to that plan.
- **Layered security** - Institutions will be expected to implement layered security for retail and business customers, that, at a minimum, must include *anomaly detection* capabilities to identify and respond to suspicions online activity. Institutions must also provide enhanced controls for administrators of commercial accounts.
- **Customer education**- The Agencies provide specific expectations the level of transparency institutions must provide to their account holders regarding protections (or lack thereof) under Regulation E.



Minimum Layered Security Expectation – Anomaly Detection

On page 5 of the Supplement, the Agencies articulate their expectations that all institutions will have the capability to detect and respond to suspicious activity and anomalous behavior. The Agencies also state that anomaly detection would have stopped the fraud cases they reviewed and clearly believe it is a capability that all institutions can affordably implement.

But what is “anomaly detection”? And how does a financial institution go about implementing such a solution? This paper offers actionable answers to frequently asked questions about what anomaly detection is and how it works to stop today’s – and tomorrow’s – online fraud schemes. The paper includes answers about deploying anomaly detection solutions, impact on in-house staff, operations, and account holders, how it actually alerts fraud analysts, and how staff, and customers, respond.

In short, this paper provides practical information for what you can actually do to meet the elevated FFIEC expectations for layered security and online fraud protection.



ONLINE BANKING FRAUD PRIMER: YOUR INSTITUTION AND YOUR ACCOUNT HOLDERS ARE UNDER ATTACK

Institutions Are Up Against Well-Funded, Organized Cyber Criminals

Understanding why multi-factor authentication (MFA) is ineffective and why the FFIEC has included anomaly detection in their recommendations starts with knowing who we're up against.

Online and mobile banking fraud is a large, sophisticated global business. Fraudsters are very organized and can be highly specialized. They work in groups and help each other, creating a powerful network that is a significantly more efficient ecosystem than our banking industry. They continually reinvest their "earnings" in advancing the technology and methods they use to defeat financial institutions' defenses.

The pace of innovation and ability to invest in attacking banks and credit unions far outweighs these institutions' abilities to invest in protecting themselves against rapidly evolving threats. Furthermore, cyber criminals have established social networks to help each other and share their most effective attacks so others can replicate their success, and they operate with explicit or implicit approval and even support of local government.

In short, by being criminals and operating outside of the laws, ethics, and procedures that guide much of the law-abiding behavior of Western financial institutions, fraudsters have a lot of advantages.

Institutions Must Protect Themselves From a Wide Array of Threats

The fraudsters' goal is straightforward: gain access to online banking accounts, set up online transactions, and transfer money undetected. The various techniques they use are all different means of accomplishing the same end. The bottom line: Banks must be prepared for any and all of the attacks.

1. PHISHING. Criminals trick account holders into unwittingly divulging their online banking credentials either online through a fake website or over the phone to a fake bank employee or automated system. Criminals have evolved their methods over time to maintain their effectiveness, and spear phishing attacks have been highly successful in targeting the executives at commercial accounts.

2. DATA BREACHES. Criminals hack into large databases to steal personal financial information for large numbers of users in one fell swoop, such as from retailers, credit card companies, and financial institutions, and then use the information to access online banking accounts. Some recent and well publicized breaches were of databases maintained by CitiGroup, Sony Playstation, Honda, Epsilon, and even the Massachusetts Department of Unemployment Assistance and Career Services.

3. MALWARE. Criminals install malware (malicious software) on the account holder's computer that enables the fraudster to implement a range of schemes. The malware is installed through email, adware, fake anti-virus schemes, and by visiting websites that fraudsters have developed to mimic well established, trusted sites, such as banks, retailers, and credit card companies.

Criminals focus their malware efforts on the weakest link – the account holder. The attacks are relentless, sophisticated, and pervasive, and can defeat most anti-virus and anti-malware software. Collectively, users don't stand a chance and education is only part of the solution. Don't get drawn into simply building stronger defenses around the user – fraudsters *will* get through them.

It's nearly impossible to avoid having malware installed on an account holder's computer when you consider:

- Results from Google image searches result in an estimated half a million referrals to fake (i.e. malware infested) anti-virus sites every day, or 15 million such referrals per week⁽¹⁾
- 71 percent of websites that have malicious code are existing, legitimate entities, not fake sites developed by the fraudsters⁽²⁾
- 81 percent of email is rigged to deliver malicious code⁽²⁾
- 95 percent of comments posted to blogs or chat forums were spam or links to malware payloads⁽²⁾



Malware is used for four general purposes, each of which is described below along with specific examples of each:

- 1) Steal credentials, including one-time passwords, to facilitate a human logging into online banking and executing fraud.
 - **Keylogging** – Malware waits for the user to log into their online banking account, and then captures the specific keystrokes that represent the user name, password, answers to challenge questions, and other essential information. The criminal then uses the information captured to log in and implement fraudulent transfers.
 - **Session Blocking** – This most commonly experienced Man-In-the-Browser attack involves malware that waits for the user to initiate an online banking session, and then captures user credentials, including one-time passwords, and passes those credentials to the fraudster in real time. The malware blocks the user session from transmitting any data to the bank (so that the one time password is not actually used) and puts up a legitimate looking “service unavailable” message. The fraudster immediately logs in from his own computer using the stolen credentials and the one-time password.
- 2) Use legitimate computer to bypass device identification, allowing the fraudster to log in from the victim’s computer and execute fraud.
 - **Machine Hijacking** – Growing in popularity, this approach uses malware to install a proxy on the victim’s device that enables the criminal to log into online banking from the account holder’s device and set up fraudulent transactions, appearing just like legitimate account holder activity. The location, ISP, operating system, IP address and other information are that of the legitimate account holder.
- 3) Use legitimate online banking sessions to execute fraudulent transactions without the knowledge of the victim. These more sophisticated Man-in-the-Browser scenarios are more rare:
 - **Session Hijacking** – Malware inserts transactions in parallel with those of the legitimate user during a live online banking session, which are inadvertently approved by the victim at the same time he’s approving his own transaction.
 - **Transaction Swapping** – Malware waits until a victim initiates a transfer and then stops the legitimate information from being sent to the institution and behind the scenes swaps out the payee and the amount. It returns a false confirmation screen back to the victim with the details of the original transaction, so all looks as expected to the victim, who then approves the transaction not knowing that it’s actually the fraudulent transaction that he’s approving.
- 4) Defeat end-user security solutions. Security companies are discovering new strains of malware that can disable secure browsing clients or even prevent them from being downloaded and installed. Another example is mobile malware that re-routes to the fraudster SMS messages containing out of band authentication passcodes so he can authorize his own transactions.

WHY ANOMALY DETECTION IS A POWERFUL FOUNDATION FOR LAYERED SECURITY

All of the fraud techniques described above – phishing, data breaches, Man-In-the-Browser – share one common element. They require some type of interaction with the online banking application to stage and execute fraud. And this is where financial institutions have the best opportunity to stop fraud attacks – by looking for unusual online banking activity. Anomaly detection provides the approach banks and credit unions need to proactively recognize account takeover and stop fraudulent attacks before the money is transferred.

Recognizing that it would have stopped fraud in the cases they reviewed while preparing the Supplement, the FFIEC Agencies now expect all financial institutions that allow external transfers or provide access to non-public personal information to have anomaly detection as a component of their layered security program.



It is a priority for the Agencies and should be a priority for all financial institutions to implement because anomaly detection:

- Defeats the widest range of threats, including all of those described above. Other layers of security are effective at what they do, but often address just one type of threat.
- Automatically protects 100 percent of retail and business users. Layers of security that must be adopted by end users result in a large portion (50 percent or more) of an account base left unprotected.
- Has no impact on customer experience and can be a tool to build trust on an ongoing basis. Many other layers of security put the burden on the account holder.
- Doesn't require account holders to install or maintain any tools, rules, or software. Other layers of security (unrealistically) require frequent updates in order to recognize new fraud threats.
- Is transparent to criminals, making it a challenge to defeat. As discussed in the malware section, other forms of security can be defeated easily by criminals.

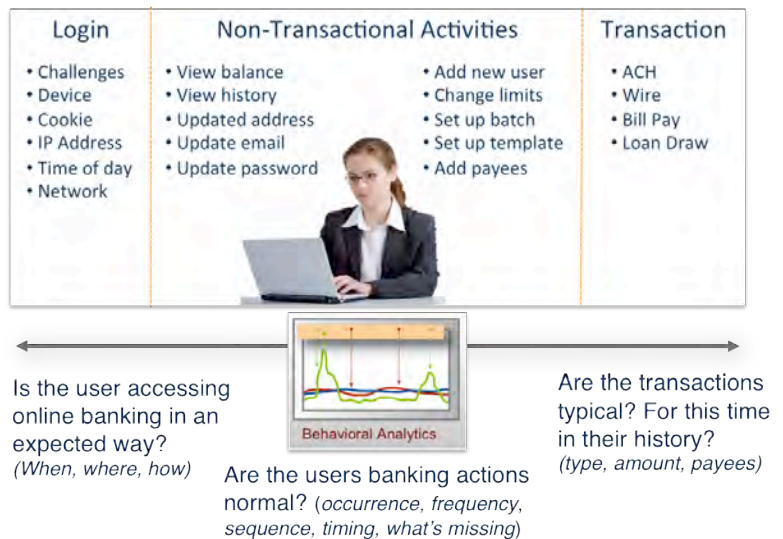
The remainder of this paper uses a Question-and-Answer format to provide the information you need about anomaly detection to determine how best to implement layered security that will meet the Agencies' expectations while protecting your account holders – and your institution – from online and mobile fraud attacks.

DETECTING SUSPICIOUS ACTIVITY: ANOMALY DETECTION BASICS

Q What is anomaly detection?

Anomaly detection is the process of detecting something unusual relative to something expected. In the world of online banking this typically means detecting unusual (or suspicious) online banking behavior in order to identify account takeover and fraudulent transactions. Examples of what anomaly detection could identify include (also see figure for additional examples):

- Accessing online banking from an unusual location or at an unusual time of day
- Using online banking features not typically used
- Using online banking features in an unexpected sequence
- Changing personal information
- Adding payees
- Adding approvers or changing approval limits
- Types and amounts of transactions





Q What is the FFIEC expecting from institutions regarding anomaly detection?

Page 5 of the 2011 Supplement says it quite clearly: the FFIEC expects **all institutions that allow high-risk online transactions to have layered security controls that include the ability to detect anomalies and effectively respond to suspicious or anomalous activity related to initial login and the initiation of electronic banking transfers.** (“High risk” is defined in the 2005 Authentication guidance as being any access to non-public personal information or funds transfer to outside parties.)

Q Why did the FFIEC choose this as a required layer of online banking security?

The Agencies explained why on page 5 of the Supplement:

“Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer’s established patterns of behavior.”

In short, the Agencies expect all institutions to have anomaly detection because it works! Anomaly detection solutions have been in place at institutions of all sizes for years and are proven to detect a wide array of online banking attacks, including the sophisticated Man-In-the-Browser attacks mentioned in the guidance (and described earlier in this paper). By using anomaly detection solutions, these institutions are able to proactively detect account takeover and stop fraud of any dollar amount before the money is gone.

Q How does anomaly detection work?

The most effective anomaly detection approach focuses on the individual account holder. Different users quite naturally have different online banking behavior from each other. Said differently, each account holder has a unique online banking fingerprint. Anomaly detection takes advantage of this fact combined with knowledge of online banking fraud attacks and general online behavior to determine if a specific online session is legitimate or has high risk of being fraudulent.

Here is simple breakdown of the process anomaly detection solutions use to detect suspicious activity for each individual account holder:

1. Create and continually update a model of expected behavior for each individual account holder.
2. Monitor every online banking session for each individual account holder.
3. Analyze all individual account behavior during an online banking session from login to logout — how they access their accounts, how they manage their accounts, the types of transactions they engage in, the frequency of activities, what kinds of activities take place during the same session, the type and amounts of payments, who the payees are, and much more (see figure on page 4).
4. By comparing individual or groups of activities in *this* online session to demonstrated patterns of normal behavior, determine if the session is legitimate or unusual, unexpected, or suspicious.

Q Is there more than one way to do anomaly detection?

Yes. Here are a few approaches to anomaly detection. Some systems rely on just one, and some use more than one approach.

- **Detection based on individual account holder behavior.** In this approach a unique baseline of behavior is established for each account holder and suspicious activities are surfaced when online behavior is unexpected for that particular account holder. Because what is unusual for one account holder may be normal for another, anomaly detection at the individual level ensures institutions are only alerted when something is actually suspicious for that individual. This approach therefore provides maximum detection with the fewest number of alerts.
- **Detection based on general or “population” level behavior.** This means looking for unusual behavior relative to an average or “typical” user, not what is unusual for a given individual. Used as



the primary method of fraud detection, this can result in missed fraud and often generates a high number of false positive alerts for an in-house team to review.

- **Detection of website traffic anomalies.** This approach seeks indications that malware is automating the process of setting up and executing transactions. For example, setting up a large number of wire transfers in a very short period, something that a human couldn't physically do that fast. This approach would not detect the most common type of fraud – a criminal using malware, phishing or data breaches to steal credentials and then manually logging in to online banking and using the online banking application as a normal human would to execute transactions.

Q Which approach does the FFIEC discuss in the Supplement?

On page 5 of the Supplement, the FFIEC points out that the fraud incidents they reviewed would have been stopped if the transfers were compared to *the customer's established patterns of behavior*. This points to a focus on individual behavior.

Additionally, in a federal court judgment on a case regarding liability for commercial account takeover and fraud, the judge cited that the bank did not act in good faith when executing over \$1M in wire transfers because the amounts, timing, and destination of the wires were all significantly different from *the customers normal banking activity*, again suggesting that an individual behavior monitoring approach is preferable.

Q The Supplement puts new emphasis on the higher risks of business banking. Should I use anomaly detection just for business banking?

The agencies expect layered security to contain anomaly detection for both retail and business accounts. Additional controls are expected for administrative functions in business accounts and as extra layers of security based on your risk assessment.

Q Is detecting anomalies in retail accounts the same as detecting anomalies in commercial accounts?

The process is generally the same, but there are a few differences in commercial banking that an anomaly detection solution should uniquely consider. These differences include the different payments types in retail vs. commercial, the dollar size and frequency of transactions, and the commercial account hierarchy – in business banking there are multiple users that both act independently and interact together using the same online account.

Q Does anomaly detection work for online and mobile banking?

Yes, anomaly detection can be used to detect suspicious activity in traditional online channels as well as mobile channels. So, it helps to address one of the perceived shortcomings of the Supplement, that it doesn't specifically address mobile banking.

Q The FFIEC wants anomaly detection at login as well as the transaction. Can a single solution cover both ends?

Yes, in fact the best approach is to look holistically from login to logout to catch anomalous activity that indicates account takeover, account reconnaissance and fraud staging before it even gets to the point of transaction. A login to logout monitoring approach yields the most complete view of online activity and provides the best context for investigation into suspicious activity. Experts like Gartner have recommended this type of "end-to-end" monitoring approach for some time. (See figure on page 4 of this paper for representative examples of all of the online activities that anomaly detection looks for from login to logout.)



HOW ANOMALY DETECTION FIGHTS CURRENT AND FUTURE THREATS

Q How does anomaly detection keep up with new strains of malware?

Anomaly detection that uses individual behavioral analytics doesn't have to. This approach is not using rules or patterns to identify specific strains of malware or attack techniques, but instead is looking for any deviation from expected behavior regardless of how the fraudster acquired the online credentials or hijacked the session. Therefore, it can automatically detect new and emerging attacks because the online behavior will still be different from the legitimate user. This addresses a criticism of the Supplement – that it is too 'backwards-looking' regarding the threats.

Q How does anomaly detection address the Zeus banking Trojan and other Man-In-the-Browser malware?

There are different types of Man-In-the-Browser malware attacks (see page 3) that use varying levels of sophistication to steal credentials and one-time passwords, login or hi-jack sessions, set up money mules, and create transactions. No matter how sophisticated a piece of malware is, a criminal still must use online banking to set up the fraudulent transfer and will do something somewhere in the online banking process that is different from the legitimate user. While it might be minor and difficult to catch with the naked eye, an anomaly detection solution can catch a single activity or combination of behaviors that are different than typical behavior.

One type of Man-In-the-Browser malware provides criminals the means to log into online banking and look as if they are doing so from a legitimate users machine in an effort to trick device identification and authentication solutions. Therefore, while there won't be any anomalies based on where they are logging in from, there will be other activities done while the criminal is logged in that won't match typical behavior. For example, the criminal could be logging in at different time and more frequently than the legitimate user does. Or the criminal might change personal information, view balances and checks in a different sequence than normal, add new payees to an ACH batch for the first time in months, or send funds of an unusual amount. Or the fraudster may leave out an activity that the legitimate user always includes, such as checking the history of recent transactions.

Q What are some real world examples of fraud attacks detected by anomaly detection?

- On April 26, 2011 the FBI, FS-ISAC, and the Internet Crime and Complaint Center [released an alert](#) on a wire transfer scheme in which the online accounts of small-to-medium sized U.S. businesses were compromised and wire transfers were sent to China – some of the transfer attempts were as high as \$1.9million. While a total of \$11million was stolen, many more transfers were attempted but caught by financial institutions that had already implemented an anomaly detection solution.
- A credit union, immediately after implementing an anomaly detection solution, identified over 100 accounts that had already been compromised, exposing them to millions of dollars in potential fraud losses. They were able to make adjustments to protect the accounts before any fraudulent transfers were even attempted.
- A national bank defeated an attack in which a fraudster used a Man-In-the-Browser scheme to hijack an online banking session, and then set up a new user with approval privileges in order to defeat dual controls. He then submitted three wire transfers totaling over \$300K over a three-day period and attempted to approve them himself using the newly added user account.
- An account holder banking with two different banks received a call from Bank 1 – that was using anomaly detection to watch for anomalous login behavior and account reconnaissance – notifying the account holder of an attempted fraudulent transfer. Suspecting the fraudster may not be limiting his attack to one bank, the account holder then contacted Bank 2 – which did not have an anomaly



detection solution in place – and learned that Bank 2 had indeed allowed a high-dollar unauthorized wire transaction to go through without realizing it was fraudulent.

Read [additional examples of customer successes](#) using anomaly detection to stop fraud.

THE PRACTICAL OPERATIONAL AND TECHNICAL IMPLICATIONS OF DEPLOYING ANOMALY DETECTION

Q Does implementing anomaly detection impact my customers or members?

No. This is the beauty of anomaly detection – it is completely transparent to your account holders. There is nothing to install and nothing to maintain, and their day-to-day online banking activity is uninterrupted by the anomaly detection solution.

Q What data supports anomaly detection solutions?

Typically an anomaly detection solution analyzes data from the online and mobile banking platforms.

Q Can an anomaly detection solution plug into a third party online banking provider?

Yes. A third party anomaly detection solution can be integrated with and used in conjunction with an outsourced online banking platform solution (Intuit, Jack Henry, Fiserv, FIS, etc).

Q What is a typical implementation time?

Implementation times vary from solution to solution, but they can be very quick and require little to no IT effort. For examples, a SaaS-based (or Cloud-based) anomaly detection solution can be implemented in a matter of a few days or a few weeks for many online banking platforms. If time is needed to customize the integration for a proprietary online banking platform or a highly customized home-grown platform, implementation time can be longer.

Some solutions are implemented on-premise and can take significantly longer and require IT resources as hardware needs to be purchased and configured, then software installed, integrated, and optimized.

Q How long does it take for the anomaly detection solution to be effective?

Anomaly detection solutions can start detecting account takeover and fraud immediately. Upon initial implementation typically there is historical data to support creating individual behavior fingerprints for each existing account holder. For new account holders, good anomaly detection solutions learn very quickly and use a variety of techniques to identify unusual activity. There are examples of anomaly detection solutions catching fraud on the very first login from a new account holder.

Q Anomaly detection sounds complicated to manage? Is it?

No. Most financial institutions use existing staff that is already assigned to fraud prevention activity in other areas of the bank or credit union. Good anomaly detection solutions will deliver a small number of alerts and rich forensic data presented in a way that allows for rapid prioritization and investigation of the highest risk accounts or sessions. Many mid-size financial institutions have less than one FTE and some spend less than one hour per day investigating suspicious activity. Larger institutions with larger account bases and higher volume of online banking sessions naturally will require more time and staff.

Anomaly detection can help financial institutions reduce staffing levels required for fraud monitoring and investigation. Institutions using anomaly detection report 50-75 percent savings in fraud monitoring, investigation, and payments review processes.



Q Is there ongoing maintenance required to keep an anomaly detection solution accurate?

Modern anomaly detection solutions do not require institutions to write rules, provide input or perform algorithm training. Some solutions do offer the optional capability of setting criteria by which the institution can more actively monitor specific categories of activity (e.g. coming from a particular fraud hotspot), but this is not necessary for the solution to be effective.

Q How does it fit in with other online banking security systems or fraud management systems I might already have in place?

Anomaly detection is the foundation of a risk-based approach to layered security. Anomaly detection solutions can gather information from other security systems, like device identification, anti-malware, secure clients, or even reputation databases to enhance its risk scoring.

RESPONDING TO SUSPICIOUS ACTIVITY

Q How do anomaly detection systems alert an institution to suspicious activity?

Anomaly detection systems notify institution staff via email or text notifications or through an alert screen in an application accessed via a browser. This can happen immediately upon the solution identifying a high-risk session or transaction.

Q How does an institution investigate an anomaly?

The anomaly detection solution should provide full details about online activity leading up to the alert, such as what activities took place, from where, for what amounts, etc. Ideally this information is presented in a way that a business user can understand and doesn't require IT staff. The fraud analyst then can look more closely into the specific account that's at risk to gather additional detail about typical activity and the recent, suspect activity.

Q What actions to banks typically take when they find an anomaly?

After doing some quick investigation to rule out any legitimate causes of the alert, institutions take one or more of the following actions (not necessarily in this order):

- Call the account holder to discuss the suspicious activity
- Put payments on hold
- Block account access
- Put the account on "high alert" for future monitoring

Q Can an anomaly detection system facilitate an automated response to suspicious activity?

Yes, at the discretion of the institution. For example, for a particular type of activity, such as a large wire transfer that is associated with a high risk score from the anomaly detection solution, the system can automatically block the transaction or shut down the online account until explicit approval has been granted. Anomaly detection can also trigger an out of band authentication action, block account access or even send a communication directly to an account holder to verify activity.



Q Does the FFIEC expect that response to suspicious activity be automated?

The FFIEC does not specify that a response must be automated nor does it specify a timeframe in which the response must occur. The response can be automated or can be performed manually. Furthermore, the FFIEC does not specify the substance of the response – i.e. does it need to be a specific answer – only that some form of response must be made.

Q What is the response from account holders when they learn there has been anomalous behavior in their accounts?

The response is very consistent regardless of whether the account has been compromised or not – the account holder is very grateful to the financial institution for proactively monitoring their account and for contacting them to verify that the specific session or transaction is legitimate. The result typically is a greater level of trust and loyalty placed by the account holder on the financial institution.

Another way to answer this question is to look at today's unfortunately all too common scenario. An account is compromised and money is stolen, and the account holder notices the loss before the financial institution does. (According to iSMG, three out of four banks were notified about a fraud loss by the account holder⁽³⁾.) So the call is from the account holder to the institution wondering where their money has gone. Receiving a call from the institution saying "your money is still safe; we're just checking to be sure" clearly is a much preferred conversation for the account holder.

ROI OF ANOMALY DETECTION

Q How do institutions typically justify anomaly detection solutions? ⁽⁴⁾

Institutions look at the following factors when calculating an ROI on an anomaly detection solution:

- **Reduced fraud losses** – anomaly detection solutions are proven to stop fraud. Institutions have prevented \$1,000 losses and \$1,000,000 losses
- **Operational savings** – anomaly detections reduce time and staff spent on fraud monitoring, fraud investigations, payments reviews, and customer outreach. Guardian analytics report 50-75% operational savings.
- **Maintain reputation** – for institutions who have not experienced significant online fraud losses, an anomaly detection solution can help to maintain their strong reputation.
- **Reduced risk associated with customer churn and lawsuits** – fraud leads to customer churn and with the recent lawsuits favoring a small business, lawsuits are expected to continue
- **Reduced risk associated with new online services** – institutions using anomaly detection have the confidence to add new online services and enhance payment service levels, knowing account holders are continually monitored.
- **Improved Customer Trust** – Account holders using anomaly detection regularly report that their customers are ecstatic with the proactive approach the institution is taking to fraud prevention.

For a complete return on investment whitepaper, contact us at info@guardiananalytics.com.

Q What do institutions that have deployed anomaly detection say about their return on investment?

Guardian Analytics customtifiers report that their solution paid for itself, and for many of them, multiple times over. The cost of a single fraud event is far more than the typical product fees for anomaly detection solutions.



SUMMARY

Anomaly detection solutions are readily available, are deployed quickly (especially SaaS solutions), and immediately and automatically protect all account holders against all types of fraud attack with minimal disruption to legitimate online banking activity. Implementing anomaly detection will not only meet FFIEC expectations, it will decrease the total cost of fraud, and will increase customer loyalty and trust.

ABOUT GUARDIAN ANALYTICS

Guardian Analytics was founded and is completely focused on fraud protection for financial services institutions. We're proud to serve banks and credit unions that are taking a proactive step to lead the way in fraud prevention. Our customers take the promise of security very seriously – it's an essential element of their brand, reputation, and their commitment to protect their institution and their account holders from fraud attacks.

Our flagship solution, FraudMAP, was developed by leveraging our employees' direct experience and deep expertise in online fraud prevention – including solving actual fraud cases – built up over many years with extensive investment in intellectual property. FraudMAP is protecting over 50 institutions and millions of account holders in banks and credit unions across the globe. www.guardiananalytics.com.

- (1) Krebs on Security, May 2011, "Scammers Swap Google Images for Malware"
- (2) Websense Security Labs Report – State of Internet Security, February 4, 2010
- (3) Information Security Media Group (ISMG) Government Information Security, published January 2011
- (4) 2010 Cost of Fraud Research, Guardian Analytics

© 2011 Guardian Analytics. All rights reserved. Guardian Analytics, the Guardian Analytics logo and FraudMAP are registered trademarks of Guardian Analytics.