A Practical Guide to Anomaly Detection

How account holder behavior can be the best indicator of account takeover and fraudulent transactions.
A Practical Guide to Anomaly Detection:
How account holder behavior can be the best indicator of account takeover and fraudulent transactions

Table of Contents

INTRODUCTION .............................................................................................................................................. 1
HOW ANOMALY DETECTION WORKS – THE HIGH LEVEL VIEW ................................................................. 1
FRAUD PRIMER: YOUR INSTITUTION AND YOUR ACCOUNT HOLDERS ARE UNDER ATTACK ..................... 4
WHY ANOMALY DETECTION IS A POWERFUL FOUNDATION FOR LAYERED SECURITY ............................. 8
DETECTING SUSPICIOUS ACTIVITY WITH ANOMALY DETECTION ............................................................. 9
BEHAVIOR-BASED ANOMALY DETECTION AND THE FFIEC ................................................................. 11
HOW ANOMALY DETECTION FIGHTS CURRENT AND FUTURE THREATS .............................................. 12
THE PRACTICAL OPERATIONAL AND TECHNICAL IMPLICATIONS OF DEPLOYING ANOMALY DETECTION 13
RESPONDING TO SUSPICIOUS ACTIVITY ................................................................................................... 14
ROI OF ANOMALY DETECTION ................................................................................................................... 15
SUMMARY ..................................................................................................................................................... 16
ABOUT GUARDIAN ANALYTICS ................................................................................................................ 17
ABOUT FRAUDMAP ...................................................................................................................................... 17
APPENDIX – FFIEC GUIDANCE ................................................................................................................... 18
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 lost dollars and damaged relationships between financial institutions and their account holders.

So far, financial institutions have responded to this complex challenge by deploying various point solutions addressing a specific threat, channel, or payment type. But, there are several key weaknesses to this approach. An alternative is to use behavior-based anomaly detection, which has proven very effective against threats that defeat these point solutions. Therefore, it is now a minimum expectation of the FFIEC, as stated in the Supplement to the Authentication in an Internet Banking Environment guidance issued in 2011.

But, what is “anomaly detection,” what makes it behavior-based, why is it uniquely effective, 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 – fraud schemes.

The paper starts with a brief definition of anomaly detection, the inherent weaknesses of point solutions, and the scope of threats against which financial institutions must defend themselves and their account holders. The paper then provides answers to frequently asked questions 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 prevent banking fraud while conforming to the elevated FFIEC guidance for layered security.

HOW ANOMALY DETECTION WORKS – THE HIGH LEVEL VIEW

Fraud doesn’t look like fraud. It looks like legitimate activity until it is compared to the normal behavior of the account holder. Every account holder has unique banking behavior, and in every fraud attack the criminal does something unusual relative to the intended victim’s established pattern.

Anomaly detection solutions dynamically build and continually update models of every individual account holder’s behavior and then detect criminal activity that is anomalous with this established norm. Anomaly detection solutions don’t require prior knowledge of a particular threat or scheme, don’t need on-going maintenance by the financial institution, and are transparent to the account holder.

In contrast, all solutions that require rules to be built do not model account holder behavior on their own but require the financial institution to define “normal.” These solutions require on-going manual maintenance of the rules, generate a high rate of false positives due to the natural scope of legitimate behavior, and only can detect attacks when the fraudulent activity is already known and has had a rule written to watch for it.

Despite the complex behavioral analytics under the surface of anomaly detection, it’s actually quite simple to explain how these solutions detect fraud and the ways in which financial institutions respond. The explanation below uses online banking to describe how anomaly detection works, although the concept is very much the same regardless of the banking channel or payment type.
1) Establish a Baseline of Individual Behavior. The first part of anomaly detection is to model the unique behavior, or “online banking DNA,” for each individual account holder – each user’s normal pattern of online banking activity. Using account holder history and ongoing monitoring, anomaly detection solutions analyze all activity from login to logout during every session and build a profile of each account holder’s normal behavior (see Figure 1).

![Figure 1: Anomaly Detection solutions start by developing a profile of each account holder’s typical behavior – their online banking DNA, if you will.](image)

2) Detect Fraudulent Activity. Enter the fraudster. Whether through phishing, data breaches, social engineering, keylogging malware, Man-In-the-Browser malware, or other means, the fraudster gains access to a victim’s account and starts to set up the fraudulent transfer (see Figure 2).

Regardless of the method used to compromise the account, the fraudster will do something during the online banking session that is inconsistent with established legitimate behavior. The anomaly detection solution will compare the fraudster’s activity, his online DNA, with what it knows about the victim’s normal behavior, and will start to flag inconsistencies. Typically, fraud is not a one-time event but a series of events from the fraudster’s initial access to the account, to reconnaissance, to possibly adding users or changing parameters, to setting up the actual fraudulent transaction. Anomaly detection involves monitoring all of this activity across all online banking sessions, resulting in a cumulative risk score that dictates when an alarm is raised.

![Figure 2: When the fraudster accesses an account, the anomaly detection solution will recognize that activity during this online or mobile banking session doesn’t match the established profile for this particular user.](image)
3) Respond to Suspicious or Anomalous Activity. When it becomes clear that a fraudster likely is behind a particular session, transaction or sequence of activities, the financial institution has several options for what action to take. The response can be automated, such as placing a hold on the account or payment, or it can be performed by a staff member, such as calling the account holder to verify the transaction (see Figure 3).

The net result is that the FI is alerted to the criminal activity before a transfer is attempted and is able to increase monitoring of the threatened account, significantly decreasing the likelihood that the fraudulent transaction will go through without notice.

Figure 3: Once the anomaly detection solution identifies a particular session, user, or transaction as possibly being fraudulent, they have total control over how to respond – automatically or through a staff member – based on full detail about the event, internal policy, the customer in question, or other factors.
In summary, the key characteristics of the most effective anomaly detection solutions are:

- They are behavior-based, not rules-based
- They automatically build and continually update models of behavior without manual updates
- They model each individual account holder’s activity instead of using a generalized model of all account holders’ activity (see related question on page 10)
- They transparently protect every account holder without requiring them to install or maintain their own defenses
- They prevent fraud by detecting difference between the fraudster’s activity and the victim’s established normal activity

**FRAUD PRIMER: YOUR INSTITUTION AND YOUR ACCOUNT HOLDERS ARE UNDER ATTACK**

Now that you have a basic concept of what anomaly detection is and how it works, let’s step back to review why it’s so important. Fraudsters are creative, organized and relentless in crafting and launching new attacks against financial institutions.

**Institutions Are Up Against Well-Funded, Organized Cyber Criminals**

Banking fraud is a large, sophisticated global business. Fraudsters are organized and can be highly specialized. They work collaboratively in groups, 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 the rapidly evolving threats. Furthermore, cyber criminals have established social networks to share their most effective attacks so others can replicate their successes. They also 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 banking accounts, set up transactions, and transfer money, all undetected. Their many techniques are simply different means of reaching the same end. The bottom line: As fraudsters have demonstrated their ability to attack anywhere, financial institutions must be prepared to defend everywhere.

Listed below are some of the more common schemes deployed by cyber criminals.

1. **Phishing / Vishing / Smishing.** Criminals trick account holders into divulging their banking credentials with seemingly legitimate emails or websites (“Phishing”), phone calls (“Vishing,” for voice phishing), or text messages (“Smishing,” for SMS phishing). Criminals have evolved their methods over time to maintain effectiveness and spear phishing attacks have been highly successful in targeting the executives at commercial accounts and bank employees.

2. **Data Breaches.** Criminals hack into large databases to steal personal financial information for a 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 banking accounts.

3. **Email Breaches.** Criminals hack into account holders’ email systems to then communicate with the victims’ financial institutions to submit a wire request or confirm a password reset, for example, and then intercept emails sent by the financial institutions to confirm transactions.
4. SOCIAL ENGINEERING. Criminals gather initial information about an account holder and then contact the financial institution personally, typically over the phone, to use what they have to learn more or to initiate a fraudulent transaction. For example, armed with an account number from a data breach plus a birth date and mailing address gathered from FaceBook, they may be able to call Client Services to reset an online banking password.

5. 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, or by visiting websites that fraudsters have developed to mimic well established and 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 (AV) and anti-malware (AM) software. Recent studies have found that because fraudsters develop new viruses and malware strains so frequently, AV and AM solutions can detect only about 5% of viruses and malware. 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.

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

A. 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 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 captured information to log in.
   • Session Blocking – This 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 one-time password.

B. Log in using the victim’s computer to bypass device identification solutions.
   • Machine Hijacking – 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, appearing just like legitimate account holder activity. The location, ISP, operating system, IP address and other information are that of the legitimate account holder.

C. Use online banking sessions initiated by the victim to execute fraudulent transactions without the victim’s knowledge.
   • Session Hijacking – Malware inserts transactions in parallel with those of the legitimate user during a live online banking session. These transactions are inadvertently approved by the victim at the same time that he is 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. It swaps out the payee and the amount behind the scenes and returns a false confirmation screen to the victim with the details of the original transaction so all looks as expected and the victim is not suspicious. The account holder then approves the transaction, unaware that it’s actually the fraudulent transaction that he’s approving.

D. Defeat end-user security solutions. Security companies are discovering new strains of malware that can disable anti-malware solutions and secure browsing clients or even prevent them from being
downloaded and installed. Mobile malware is another example; it re-routes SMS messages containing out of band authentication passcodes to the fraudster so he can authorize his own transactions.

**Attacks Take Many Paths from Account Compromise to Payment**

The diagram below puts these threats into a larger context to show the many ways that a fraudster can successfully navigate from a specific type of attack to moving money through a number of different payment types. As mentioned earlier, because fraudsters can attack anywhere, financial institutions must defend everywhere.

Figure 4 shows the four components that are present in a fraud attack:

1. **Method of Compromise** – These are the various schemes described above that fraudsters use to compromise an account.

2. **Point of Compromise** – Fraudsters initially focused on compromising online banking accounts, but have quickly expanded their attacks. The extremely fast growth of mobile banking has attracted fraudsters’ attention. Fraudsters also target call centers, the account holders themselves (e.g. with vishing attacks), and recently have included bank employees in their sights as they attempt to get direct access to payment systems such as the wire payment system.

3. **Channel for Money Movement** – Once they’ve compromised an account, the fraudster has numerous options for moving the money out. They can instigate online payments, have a call center rep initiate a wire payment on their behalf, or target a branch location.

4. **Payment Type** – Finally, each channel offers a variety of payment types.

---

Figure 4: Fraudsters use a range of techniques and channels to access victims’ accounts, and use a variety of channels to get the money out, introducing many combinations of these that must all be guarded against by financial institutions.
Multi-Channel Threats – Endless Fraud Scenarios

There was a time when fraudsters would do everything in one channel. They would log into an online banking account, for example, complete the necessary reconnaissance, set up the attack, and attempt a fraudulent transfer, all from within the single online account. This led some FIs to implement narrowly defined point solutions designed to stop one particular type of attack or protect one specific channel.

However, fraudsters have demonstrated an increasing ability to combine communications and banking channels in a single attack. The number of possible paths through the diagram above represent the endless number of scenarios that fraudsters can deploy, and therefore show how deeply financial institutions must be prepared to monitor, detect and respond. For example:

- The fraudster uses a phishing scheme to steal credentials, logs into online banking to view check images, and then attempts to cash forged checks.
- The fraudster uses credentials gained in a data breach to access online banking, and then uses the online chat feature and social engineering skills to have the client service representative submit a fraudulent wire transfer request.
- The fraudster compromises the victim’s email system, submits a wire request online, and then intercepts the confirmation email to approve the transfer.

The impact on financial institutions is that they need to detect suspicious activity wherever it occurs and before a transaction has been attempted because the transaction itself could be attempted in a completely different channel.

The response to the complex challenge so far is that institutions have deployed various point solutions addressing either a specific threat, channel, or payment type. For example, institutions have implemented device ID solutions to prevent a compromise to the online channel, tokens to validate online payment requests, and transaction-monitoring solutions to detect suspicious wire payments. This is a reasonable evolution that delivers incremental progress over time. However, there are challenges with how this evolution has played out.

First, these point solutions are often too narrow in scope. They may solve a particular problem and do it well, but they will be blind to vulnerabilities in other systems and sometimes, even those within the same system they are protecting. Anti-malware solutions, for example, are vulnerable to other criminal account-hacking methods and don’t assist with protecting other channels outside of online banking.

The second challenge is that point solutions are often fixed and static. They don’t evolve with the threats fast enough and can’t adapt to problems beyond what they were designed for.

The third problem, and probably the largest, is that most of these solutions exist in isolation and don’t work together well, if at all. For example:

- A borderline transaction might be approved by a transaction-monitoring solution, but that same transaction taken in context with a highly unusual change to the account password would generate a much higher risk score.
- A high-dollar payment might always require out-of-band confirmation. However, if that payment is consistent with a standard weekly payment that a client has been making for a long time, then the risk is actually very low. Forcing an OOB confirmation is actually very poor customer service in this case and distracts operations staff from higher risk activities.

As a result, these solutions aren’t as effective as they could be. They don’t really address the complexity of the threats in the context of a financial institution’s individual environment. This makes it easier for criminals to identify new gaps.
WHY ANOMALY DETECTION IS A POWERFUL FOUNDATION FOR LAYERED SECURITY

All of the fraud techniques described above share one comment element – they require some type of interaction between the criminal and the financial institution to stage and execute fraud. And this is where financial institutions have the best opportunity to stop fraud attacks. Anomaly detection provides the approach banks and credit unions need to proactively recognize account takeover, reconnaissance, and fraud setup, and stop fraudulent transactions before the money is gone, regardless of the point of compromise, channel, or payment type.

By focusing on behavior, anomaly detection solutions can prevent new threats and schemes with no advanced knowledge of how the scheme works, what malware is used, and whether it’s a manual or automated attack. Whatever the scheme, at some point the fraudster will diverge from the victim’s normal behavior.

What is needed to effectively prevent fraud is a solution that’s agnostic to the threats, takes an expansive view of account holders and the actions they take when interacting with the institution, and can factor in and take advantage of the solutions that are already in place. Anomaly detection solutions:

- Defeat the widest range of threats, including all of those described earlier. Other layers of security are effective at what they do, but often address just one type of threat.
- Automatically protect 100 percent of retail and business account holders. Layers of security that must be adopted by end users (such as anti-virus or anti-malware software) result in a large portion (50 percent or more) of an account base left unprotected.
- Have no impact on the account holder’s banking experience and can be a tool to build trust on an ongoing basis. Some security solutions put the burden on the account holder or make the banking experience more complicated or time consuming.
- Don’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.
- Can utilize data provided by point solutions to enhance the behavioral profile created for each account holder.
- Are transparent to criminals, making them a challenge to defeat. As discussed in the malware section, once fraudsters detect a particular security solution is in place, they have demonstrated their ability to defeat them.
DETECTING SUSPICIOUS ACTIVITY WITH ANOMALY DETECTION

What specifically does anomaly detection look at to detect online and mobile banking fraud?

Anomaly detection is the process of detecting something unusual relative to something expected. To do so, anomaly detection solutions monitor and analyze everything that goes on from login to logout, and then compare it to previously demonstrated norms. This includes what the user (or fraudster) is doing, from where, at what time of day, and so forth. But, perhaps less obvious, it also looks at what typically is done that may be being skipped this time, what is absent that is normally present.

Examples of what anomaly detection could identify include (also see figure for additional examples):

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

How does anomaly detection work?

The most effective anomaly detection approach focuses on the individual account holder. Different users quite naturally have different banking behavior. Said differently, each account holder has a unique banking fingerprint.

Here is a simple breakdown of the process used by anomaly detection solutions 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 banking activity for each individual account holder, including through the online and mobile banking channels and requests for different types of payments (e.g. ACH or wire).
3. Analyze all individual account behavior: how they access their accounts, when and how often, 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 above).
4. Compare current behavior to historical patterns of normal behavior to determine if the activity is legitimate or unusual, unexpected, or suspicious.
5. Issue alerts for high-risk sessions or activity.
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 surface when 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 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 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 very 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.

How is anomaly detection different from rules-based solutions?

Anomaly detection solutions dynamically and continually update models of individual account holder behavior, comparing new activity to these established models. They don’t require any knowledge of the fraud scheme in play and will automatically update behavioral models as account holders change how, when, and from where they bank. Rules-based solutions require prior knowledge of what the FI is looking for so it can write a rule to detect it. The challenges with rules-based solutions are that they require constant maintenance and updating, generating a lot of work for the FI, and fraudsters are continually changing their attack schemes, so rules-based solutions will always be a step behind and will miss the latest scheme that the fraudsters have launched.

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 payment 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 account.

Does anomaly detection work for online and mobile banking and across different payment types?

Yes, anomaly detection can be used to detect suspicious activity in any electronic banking channel, including online and mobile, and regardless of the payment type, including ACH, wire, and online bill pay.

It seems like more and more companies are offering anomaly detection solutions. Are they all similar, providing the same functionality?

Developing an anomaly detection solution requires sophisticated, complex mathematics and it can take many years to ensure it is effective, easy to use, does not change the account holder’s banking experience, and does not generate a large number of false positives that require time-consuming follow-up by bank...
personnel. Compelling and effective solutions have been available for many years from vendors specializing in behavioral analytics and anomaly detection. However, when the updated FFIEC Guidance came out specifically calling for anomaly detection, several vendors announced anomaly detection capabilities that have been added onto their existing solution. Given the complexity of the software, it’s hard to imagine that a company that has specialized in other aspects of online banking could also have the expertise needed to create a viable anomaly detection solution. Financial institutions are encourage to ask vendors about core competencies, expertise, and proof points that substantiate their claim to have rather suddenly developed a solution that very reasonably takes many years to perfect.

**Behavior-based Anomaly Detection and the FFIEC**

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

Page 5 of the 2011 Supplement (see Appendix) says it quite clearly: the FFIEC expects all institutions that allow high-risk online transactions to have layered security controls with 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.)

**Why did the FFIEC choose this as a required layer of electronic 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 fraud threats, 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 before the money is gone.

**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.

**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.

**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 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 9 of this paper for representative examples of all of the activities that anomaly detection looks for from login to logout.)

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 performed manually. Furthermore, the FFIEC does not specify the substance of the response, only that some form of response must be made.

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 about using rules or patterns to identify specific strains of malware or attack techniques, but instead, it is looking for any deviation from expected behavior regardless of how the fraudster acquired the credentials, initiated a payment, or hijacked the session. Therefore, it can automatically detect new and emerging attacks because the behavior will still be different from the legitimate user.

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 5) 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 from typical behavior.

One type of Man-In-the-Browser malware provides criminals the means to log in to online banking and appear as if they are doing so from a legitimate user’s 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 times of day 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?

- In 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 $1.9 million. While a total of $11 million 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 as indicated by anomaly activity but no transactions yet, 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 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.

A fraudster used stolen credentials to log into online banking and then used the online chat feature to ask for help with a wire transfer. Anomaly detection spotted the anomalous first-time use of the chat feature and of sending a wire.

An account holder banking with two different banks received a call from Bank 1 – which 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.

THE PRACTICAL OPERATIONAL AND TECHNICAL IMPLICATIONS OF DEPLOYING ANOMALY DETECTION

Q Does implementing anomaly detection impact my customers or members?
No. It is completely transparent to account holders. There is nothing to install and nothing to maintain, and their day-to-day banking activity is uninterrupted by the anomaly detection solution.

Q What data supports anomaly detection solutions?
Anomaly detection solutions analyze data from a number of systems that a financial institution uses to provide various services. For example, they can analyze data from the online and mobile banking platforms as well as the FI's ACH and wire systems.

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 or a mobile banking platform. Typically, anomaly detection solutions do not need to be integrated with the core banking platform.

Q What is a typical implementation time?
Implementation times vary, 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 several weeks for many online banking platforms. If time is needed to customize the integration for a proprietary online banking platform or a highly customized homegrown 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 begin creating individual behavior fingerprints for each 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.
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 banking activity 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.

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

Advanced anomaly detection solutions do not require institutions to write rules, provide input or perform algorithm training. Some solutions do offer an optional capability to set 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.

How does it fit in with other 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

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

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

How does an institution investigate an anomaly?

The anomaly detection solution should provide full details about the 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 details about typical activity and the recent, suspect activity.

What actions do financial institutions typically take when they find an anomaly?

Financial institutions always start by investigating an alert to rule out any legitimate causes. For activity that generates a high risk score and remains suspicious after some investigation, the institution can take one or more of the following actions (not necessarily in this order), always maintaining complete control over the timing, method, and content of any contact with the account holder:

- Call the account holder to discuss the suspicious activity
- Put payments on hold
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, the system can automatically block the transaction or shut down the 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.

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 in 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 an iSMG survey, three out of four banks were notified about a fraud loss by the account holder.) 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” is clearly a much-preferred conversation for the account holder.

ROI of Anomaly Detection

How do institutions typically justify anomaly detection solutions?

Based on the results of a Guardian Analytics Cost of Fraud survey, institutions look at the following factors when calculating an ROI on an anomaly detection solution:

- **Fraud losses** – Anomaly detection solutions are proven to stop fraud. Institutions have prevented $1,000 losses and $1,000,000 losses.
- **Operational savings** – Anomaly detection solutions reduce time and staff spent on fraud monitoring, investigations, payments reviews, and customer outreach. Guardian Analytics reports 50-75% operational savings.
- **Brand reputation** – Few events tarnish a financial institution’s reputation like a fraud loss. An anomaly detection solution can help to maintain a strong brand reputation.
- **Customer churn and lawsuits** – Fraud leads to customer churn, and with the recent lawsuits favoring the account holder, lawsuits are expected to continue.
- **New banking services** – Institutions using anomaly detection have the confidence to add new services, enhance payment service levels, and expand use of current revenue-generating services, 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, building trust and loyalty.
What do institutions that have deployed anomaly detection say about their return on investment?

Guardian Analytics customers 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, deployed quickly (especially SaaS solutions), and will immediately and automatically protect all account holders against all types of fraud attacks with minimal disruption to legitimate 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.

FraudMAP was developed by leveraging our employees’ direct experience and deep expertise in fraud prevention – including solving actual fraud cases – built up over many years with extensive investment in intellectual property. FraudMAP is protecting nearly 300 institutions and millions of account holders in banks and credit unions across the globe. [www.guardiananalytics.com](http://www.guardiananalytics.com).

ABOUT FRAUDMAP

FraudMAP behavior-based anomaly detection solutions enable banks and credit unions to leverage the most important advantage they have over cyber criminals – deep knowledge of individual account holder behavior. Using patented transaction and behavioral monitoring capabilities plus easy to use investigation tools, FIs use FraudMAP to proactively identify account takeover, account reconnaissance and fraud setup, and fraudulent ACH, wire, bill pay, and other transactions before money is transferred. It also enables financial institutions to conform to the FFIEC’s expectations for layered security that includes anomaly detection (see chart).

FraudMAP instantly and automatically protects all business and retail account holders from the widest range of existing and emerging threats with minimal inconvenience or disruption to their legitimate online banking activity. As a Software-as-a-Service (SaaS) solution, FraudMAP is low cost to deploy and no cost to maintain. Institutions can deploy FraudMAP quickly with little to no support from IT.

Guardian Analytics offers purpose-build versions of FraudMAP for various banking channels and payment types:

- FraudMAP Online for Retail Banking
- FraudMAP Online for Business Banking
- FraudMAP Mobile
- FraudMAP ACH
- FraudMAP Wire
- FraudMAP Access
APPENDIX – FFIEC GUIDANCE

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 account holders. 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 at least every 12 months or as the internal and external environment changes. Institutions are expected to 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 clients that, at a minimum, must include anomaly detection capabilities to identify and respond to suspicious activity. Institutions must also provide enhanced controls for administrators of commercial accounts.
- **Customer education** – The Agencies include specific expectations for 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.

**Applies to More than Just Online Banking**

The initial interpretation of the Guidance was that it only applied to online banking. This has since been clarified through various comments made by the Agencies. The guidance, when read literally, references “Internet banking” (see the title of the Guidance, for example) and “electronic banking.” For example, page 5 reads, “Layered security controls should include processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to: 1) initial login and authentication of customers requesting access to the institution’s electronic banking system; and, 2) initiation of electronic transactions involving the transfer of funds to other parties.” Accordingly, the Guidance applies to both online and mobile banking channels, and all types of electronic transactions, including ACH, wire, and bill pay.