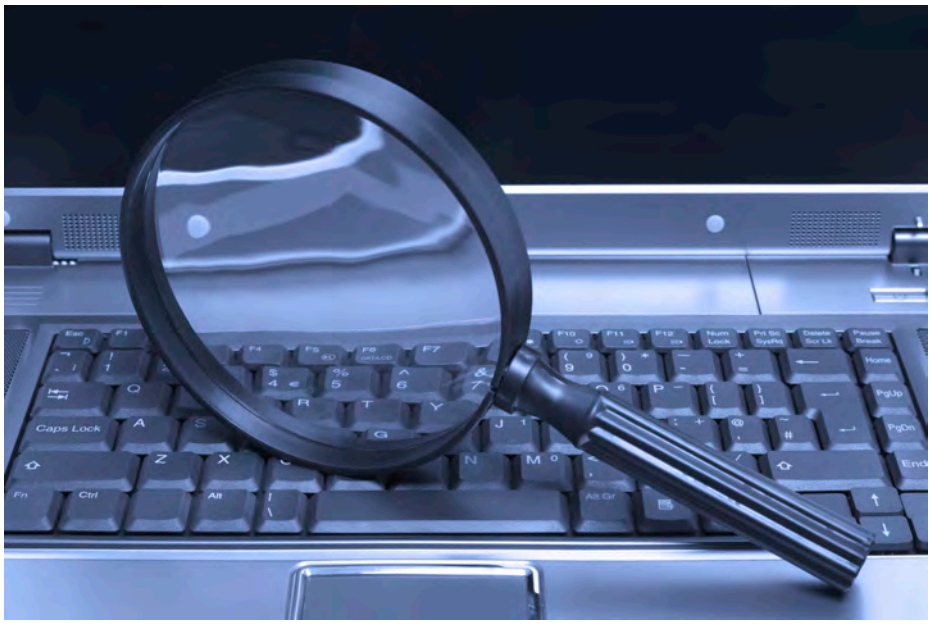
Guardian Analytics

Best Practices for Detecting Banking Fraud



White Paper

Guardian Analytics

Best Practices for Detecting Banking Fraud

Table of Contents

INTRODUCTION 1

OVERALL FRAUD PREVENTION STRATEGIES 1

MONITORING ACCOUNT HOLDER BEHAVIOR 3

- DEVICES AND LOGIN ACTIVITY 3
- ISP & IP ADDRESS 4
- DURING A SESSION 6
- ACROSS SESSIONS / SEQUENCE OF SESSIONS 7
- ACROSS CLIENTS 7

HOW TO DETECT AUTOMATED ATTACKS THAT USE MAN-IN-THE-BROWSER 8

BUSINESS PRACTICES FOR BANKING OPERATIONS 9

ANOMALY DETECTION 11

CONCLUSION 12

ABOUT GUARDIAN ANALYTICS 12

INTRODUCTION

Banking fraud is a sophisticated global business. Cyber criminals are organized, coordinated, and highly specialized, thus creating a powerful network that is, in many ways, a significantly more efficient ecosystem than our own banking industry. They continually reinvest their "profits" to advance the technology and methods they use to defeat the layers of security financial institutions (FIs) have put in place.

Fraudsters' pace of fraud innovation and their ability to invest in attacking banks and credit unions far outweighs these institutions' abilities to invest in protecting themselves against rapidly evolving threats. Whether it's phishing scams, mobile malware, banking Trojans, Man-In-the-Browser schemes, or the many techniques for bypassing multi-factor authentication, threats span online banking, mobile banking, as well as the ACH and wire payments channels. The range and sophistication of the threats against which financial institutions must defend themselves continues to grow.

To effectively combat the cyber criminals FIs must be at their best, learning from those who have demonstrated success. Guardian Analytics fraud analysts collectively have nearly 50 years of experience fighting fraud every day. This white paper presents a range of strategies and techniques they have developed and proven in day-to-day battles with fraudsters. While there are many specialized cases, each of which could be covered in far greater detail, we have kept these best practices at a somewhat higher level in order to keep the entire paper to a reasonable length.

The paper begins with overall strategies for preventing fraud, covers specific tactics for detecting fraud while account holders are engaged in online or mobile banking, describes operational strategies that will help financial institutions to respond quickly and effectively when fraudsters strike, and concludes with a description of anomaly detection as a category of fraud prevention solutions that are designed to implement many of the best practices described in this paper.

OVERALL FRAUD PREVENTION STRATEGIES

The following broad, guiding principles will provide context for the more specific fraud detection techniques discussed later in this paper.

Know your customers – Knowing who your customers are, what business they're in, and the purpose for which they have a bank account (e.g. business, personal, education, savings, etc.), provides a valuable initial context for any electronic banking transaction. The added benefit is that the more you know about your customers, the better you will be at providing them with the services they need and want.

Monitor all activity from login to logout – Fraud doesn't just happen at the transaction. It is an on-going process that typically plays out over a period of time during which the fraudster gains access to the account, does some reconnaissance, sets up the attack, and then executes the fraudulent transactions. Monitoring all online and mobile banking activity from login to logout yields the early fraud indicators so you can intervene well before a transaction is attempted.

Be proactive; don't wait for the transaction – Research conducted by the Ponemon Institute in 2012 found that the number one way in which FIs discovered fraud attacks was when their clients contacted them after noticing money was missing from their accounts. That is the common scenario when an FI is reactive, merely waiting for something to happen and dealing with the problem after a loss occurs. If you are waiting for the "fraudulent transaction" alarm to sound, you will probably be too late. Truly preventing fraud, not just recovering or replacing stolen funds, requires a proactive mentality that is looking to preempt the fraud scheme early in its development.

Being proactive includes identifying "sleeper" accounts that have already been compromised but have not yet been used for fraud, monitoring accounts and questioning abnormal activity, investigating suspicious behavior, and taking action such as contacting the account holder well before the fraudster actually attempts to move money. You don't know how a fraud attack will come. So, ignoring suspicious behavior because there's no money movement leaves the FI open to a later fraud attack—possibly in a different channel. Instead, the best approach to protect against fraud is to take action when you first see an anomaly that could indicate account compromise.

When you discover a compromised account, it is initially difficult to discern how the account was actually compromised, so you must investigate all possibilities—have the account holder check the computer for viruses, check with credit bureaus, change login credentials, issue a fraud alert with credit bureaus. Do everything possible to decrease the risk of the account being compromised again.

Look for inconsistencies with previously demonstrated "normal" behavior – This is called "anomaly detection," which is a well-established, analytical technique for identifying unexpected or unusual behavior relative to previously established patterns of normal behavior (see page 11). In order to commit banking fraud, cyber criminals must at some point access the online banking account to gather information, set up an attack or initiate a fraudulent transaction, and when they do, they will do something that is unusual or unexpected in the context of your real client's typical banking behavior. The power of using anomaly detection lies in the fact that it doesn't matter how the account is compromised – whether it's a Trojan or other malware, stolen credentials, or social engineering through customer service – the suspicious behavior relative to established norms is what provides a clue or signal that something is amiss.

Focus on the individual account holder, not "average" behavior – Some anomaly detection solutions use generalized or "population" level data for what constitutes "normal" behavior. But "normal" for one person may be completely unusual for another. For example, one client may travel a lot and is frequently accessing his account from a number of different locations, while another only uses online banking from home. Or, one client may frequently wire tens of thousands of dollars while another uses online banking only for paying household utility bills that seldom exceed $100. Always consider what is typical or previously demonstrated activity for *this* particular account holder to decide if activity during *this* session is suspicious or not.

Use layered security – There is no silver bullet when it comes to fraud prevention. Whether it's device ID, tokens, out of wallet challenge questions, out of band authentication, or positive pay, fraudsters have found a way to get past each of them. But it is extremely difficult to get past ALL of them. A layered security strategy, as called for by the FFIEC, means that when (not *if*, but *when*), the fraudster gets past one layer, another confronts him. Each layer adds to the effectiveness of the entire security strategy.

Don't assume that account holders are doing what they need to do to protect themselves – As per earlier comments about layered security, it's good to have an anti-virus (AV) software and a layer of security provided by a dedicated, secure computer. But clients will at some point cut a corner, or fail to update their AV software, or log in from home "just this once," which bypasses in-house security and firewalls and opens the computer up to malware. FIs must base fraud prevention strategies on the assumption that the end point is compromised, which applies equally to commercial and retail accounts.

Stay vigilant – A boxer can't let down his guard because it only takes a moment for his opponent to see an opening and land a knockout punch. The same is true with fraud prevention. Perhaps you've just implemented a new technology solution that significantly improves your detection capabilities. You still do not have the luxury to believe for a moment that now the financial institution is safe. The fraudsters are continually updating their schemes, reacting to new defenses, and creating new capabilities.

Staying vigilant includes maintaining a broader perspective on what is going on at your institution and in the marketplace. Have what is called "situational awareness" to know, for example, if a particular scheme is suddenly appearing more often and therefore would cause you to increase overall alert level or monitor particular accounts more closely. Alternatively, if your corporate website suffers a distributed denial of service (DDoS) attack, even if it doesn't directly impact your online banking capabilities, it might actually be serving as a smokescreen for soon-to-follow banking fraud attack (as we've seen repeatedly).

Monitoring Account Holder Behavior

This section includes specific tactics for detecting potentially fraudulent activity. It is organized around different phases or aspects of the online banking process, as shown in Figure 1.

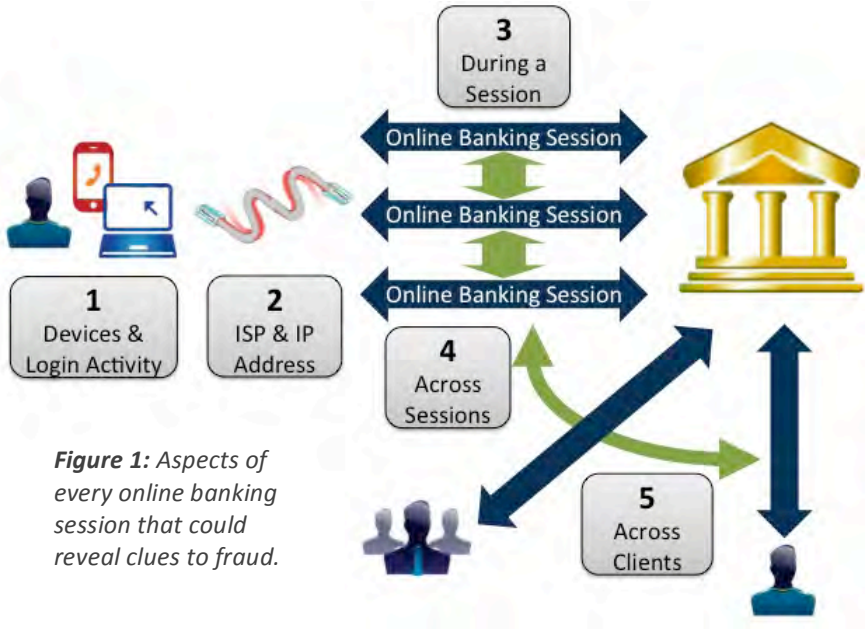


Figure 1: *Aspects of every online banking session that could reveal clues to fraud.*

1. Devices & Login Activity

At login, check to see if the device being used is consistent with the device typically used to log into this account. If not, is there a logical explanation for the discrepancy?

However, it might be that a Man-In-the-Browser (MITB) attack is underway in which case the fraudster appears as the legitimate user from a device perspective.

Recently fraudsters have demonstrated the ability to copy device settings onto a virtual PC, which will fool fraud prevention solutions that look primarily at device information. So while a device that appears to be legitimate is not necessarily sufficient to declare the session safe, seeing some kind of change in the device definitely is something worth investigating.

Some of the other data points you might check at this stage are:

- Is the time of day at which the login occurs typical as compared to past login history?
- Does the login process take longer than usual, or does it take several tries where as typically the user is always able to access the account on the first try?
- Is the account holder using the "Forgot my password" feature for the very first time? This is a common fraudster technique for resetting passwords.
- Was a challenge question answered incorrectly?

A fraudster may still be successful in logging in, but any difficulties in doing so could be a clue that this is not the legitimate account holder.

2. ISP, IP Address, and Geolocation

When looking for consistent behavior by the account holder, one data point that is always present in every online banking session is the Internet Service Provider (ISP) and IP address. Comparing these to established patterns is an important part of evaluating every online session.

Another use of ISP and IP information is to attempt to determine the client's location. Are they logging in where they typically access online banking? However, using IP address or ISP information to determine location is often not the best indicator of a customer's login location – it's somewhat like using someone's mobile phone area code as an indicator of where they are at that moment. An IP address gives an approximate location that's generally reliable at country, less so at the state level, but questionable at the city level because it's the location of where the data exits the ISP and not where the account holder is sitting.

Your greatest advantage is to know many aspects of your customers' behaviors, and as you learn more about different ISP providers, ISP and IP address information can provide a helpful clue in the overall behavioral context.

ISP – Generally speaking, if the ISP has been consistent and then it changes, that's suspicious and is worth further investigation. However, some fraud attacks are launched through the victim's computer, in which case the ISP will look normal. Therefore, a consistent ISP, by itself, is not sufficient to determine that an online banking session is legitimate.

Determining the location of the account holder is made possible through the IP address, which is a function of the ISP but is not something that can be discerned simply by knowing what ISP is being used for a particular session.

IP Address Types

Understanding IP Type is extremely important and it will assist with determining what actions to take based on what you are reviewing. Depending on the category into which the IP address falls, you will either put more or less weight on the location.

a. **Normal** – Provides a specific and consistent IP address for the connected device. These are fixed-line connections so the user will be at or near the normal location. Examples include cable companies and DSL providers.

b. **Proxy Server**. In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients (users) seeking resources from other servers (e.g. websites). A client connects to the proxy server, requesting some service or resource available from a different server (such as a web page), and the proxy server delivers the requested digital asset. Given this middleman role, a proxy server is not a reliable source for geolocation information.

   Types of proxy servers include:

   - Mobile Gateway. This connection uses a gateway to connect a mobile device to the public Internet, and location can vary. Examples of mobile ISPs that use proxy IP addresses are Blackberry, Verizon Wireless, and AT&T Wireless. Looking at location information for mobile ISP provider often shows a different location than where the user actually is due to the nature of mobile devices and people traveling. These providers always makes it look like the account holder is "home." Also, the actual time of the online or mobile banking session can be misrepresented given time zone changes; e.g. time at "home" may be what's recorded when in reality the user is in a different time zone.

Best practice when it comes to ISPs is simply to pay attention and over time, after investigating more and more suspicious sessions, a fraud analyst will start to recognize some ISPs and their characteristics, such as if they're mobile, or a cable carrier, or international.

IP Address – As with the ISP information, a consistent IP address followed by a change in IP address is suspicious. However, a frequently changing IP address provides no clues as to whether the session may be fraudulent or not.

Only in select cases can an IP address provide accurate location information because IP addresses are not hard-wired to a specific country or region.

Some IP addresses are dynamically assigned, so they're different with every session, while others are dedicated and therefore never change. ISPs offering Normal IP addresses (see sidebar) can move entire blocks of IP addresses geographically, so even seeing a change relative to what had been a consistent IP address still is not a definitive indicator of fraud.

All in all, the IP address is not a particularly reliable indicator of location, and a new IP address may, or may not, be suspicious. In some cases, though, it can be an indicator that further investigation is prudent.

See the sidebar for a description of different types of IP addresses. These are important to understand to help you to recognize situations where the IP address provides relevant information, and when it doesn't.

IP Address Types (cont'd)

b. Proxy Server (cont'd)

- International Proxy. This connection routes traffic from multiple countries and are popular within corporate networks.
- Regional Proxy. This connection routes traffic from multiple states or provinces within one country and again are popular within corporate networks.
- Satellite. This connection is via a consumer satellite, which can span a continent or more and provide various locations.

c. **Proxy Anonymous** – Uses an anonymous proxy server that hides the identity of the connected device. This will show up as type "Proxy Anonymous." And while it does not necessarily mean it's fraud, you must take into consideration that you really don't know the identity of this particular connection. Sometimes this is the result of the account holder intentionally encrypting their location, such as when someone has been the victim of identity theft. In this case, however, the ISP and IP address will always be different, so this in and of itself becomes a consistent behavior pattern.

d. **Aggregator** – Provided by an account aggregation service that enables Internet or network access to multiple accounts from the Aggregator's dedicated IP addresses. When an aggregator is being used, do not draw any conclusions about location or the time of the banking session. Some examples of aggregators are CashEdge, Digital Insight Corporation, Mint, Peak Web Hosting, and Yodlee.

e. **Reserved** – Private IP addresses are often used by internal corporate networks and they provide no information that can be useful. The location, IP address, and other data is shown simply as "unknown." However, this should be very consistent across sessions.

There are online services into which you can enter an IP address and it will provide IP type, ISP, and other information that may be helpful. Some examples are MaxMind, DNS Stuff, and Info Sniper.

3. During a Session

The specific activity that takes place during an online or mobile banking session will provide a lot of clues about who is actually online. Best practice at this stage is simple: if something does not look right, be proactive and investigate the session further.

Here are some specific aspects of every online session that are worth watching carefully. While none of these are necessarily clear and consistent indications of fraud, together they can help to detect suspicious activity that may be indicative of a fraud attack.

- Look to see if activities are similar to earlier sessions or are they new. For example, is the "view check images" feature being used for the first time (which fraudsters use to get signatures)?
- Look for the sequence of activities within a session. For example, does that account holder always check her balance before requesting a transaction?
- Look for profile modification activities, which generally happen infrequently. These could include changing the email address, phone number, security and alert settings, approval limits, or adding a new user.
- Consider the length of time in the session. Legitimate users typically log in, do something, and then log out. They're on a mission. Fraudsters might stay longer and snoop around a bit to do some reconnaissance.

<u>At the Transaction</u>

While this is late in the fraud attack, it is still very important to monitor all transaction activity. Look for:

- Transaction Types. For example, if an account holder historically only has used online banking for bill pay and now is submitting his first request for a wire transfer.
- Unusual amounts. These need to be evaluated in the context of each account holder's prior activity. For example, setting a rule that triggers a manual review of every transaction that's over $10,000 doesn't make sense given that this may be common for some account holders and very unusual for others. Such rules tend to trigger a lot of false positive high-risk alerts, creating unnecessary work for employees at the financial institution. It also does not make sense to set the limits at $1 which forces every transaction to be reviewed and further exposes all transactions to prying eyes by asking account holders to answer challenge questions or to provide other confirmation details that can be captured and reused by fraudsters.
- Inserted or modified line items in ACH batches.
- New payees.
- Unusually rapid timing between submission and requested close. For example, requesting a same day close vs. the more typical 3-day close for ACH transactions.
- Wire transfers are extremely popular with fraudsters because of the speed with which they're executed and the how difficult they are to reverse. One clue to look for is how the wire is requested. For example, does the account holder typically use a template but in this session is using a free-form request to submit a wire transfer. Also, check the dollar amount of the wire, which for fraudulent transactions typically will be different than what has been seen previously for this client.

4. Across Sessions / Sequence of Sessions

There may be some similarities in the activities that take place in every session, regardless of device or location. This could include time of day, day of the week, duration of the session, or combinations of transactions and timing, such as always using online bill pay early in the month.

- Always check the session immediately prior to the session in question (and the session afterwards, if there is one available). Ask yourself, "Does this sequence of activities across the sessions make sense?" For example, the fraudster might happen to log in between two legitimate sessions, and the sequence of activities across all three will look odd.
- Look at the time delay between sessions in the context of location. Is the time/distance combination possible? For example, the user logged in from California, and then 2 hours later logged in from New York. If the combination is not physically possible, is there a logical explanation? For instance, is someone logging in to help a parent who lives in another part of the country, or is a spouse logging into the same account from a different location due to business travel, or is someone using a corporate VPN that may be rerouting Internet traffic?
- Consider activities in context of other recent activity. For example:
    - A customer reviewing a history of bill pay transactions may not, in and of itself, be unusual. However, it could be suspicious if the account holder just did this yesterday, and is now checking it again today.
    - Is it normal for the account holder to log on multiple times in a given day? Using different ISPs?
    - The account holder changes his password, and then in the next session has trouble logging in. This could indicate that a fraudster changed the password and then the victim tried to log in with the old password.

5. Across Clients

When fraudsters find a weakness in a financial institution's layered security approach, they will often use it against several accounts simultaneously or in rapid succession. So, when fraud is discovered in one account, best practice is to look for attacks with similar characteristics against other accounts.

Another suggestion is to consult peers at other institutions to see if they have experienced the same attack. Fraudsters have been known to launch simultaneous attacks against multiple institutions that all use the same online banking platform. Working cooperatively with peers can help all institutions to detect these larger scale attacks.

How to Detect Automated Attacks That Use Man-In-the-Browser

Detecting automated attacks and Man-In-the-Browser attacks can be particularly challenging, especially when they're combined. Device and location information will look legitimate because the session is coming through the victim's own computer. But there will be anomalies when compared to the full complement of normal account holder behavior.

To detect Man-In-the-Browser attacks, look at payees and dollar amounts for inconsistencies as compared to prior transactions. Also, look for sequence of activities and possibly what is missing that is typically present in a legitimate session. (See Business Banking example in sidebar.)

For automated attacks, timing is a critical factor. The fraudster's timing of activities will generally be different from the legitimate user's, even if the fraudster has programmed the automated attack to try to simulate natural human timing patterns. The speed with which activity takes place, be it unusually fast or slow, can indicate an automated attack.

Automated attacks, whether using MITB or not, will also tend to have inconsistencies in regards to payees and transaction amounts or other characteristics of the transaction such as requesting a 1-day close for an ACH payment.

Examples Of How Best Practices Can Detect Actual Fraud

These are examples of actual attacks that demonstrate characteristics of fraud that can be detected using the best practices described in this paper.

Retail Banking

The established normal behavior for this account holder is to always bank from the same location, from the same machine, with online transactions limited to hundreds of dollars. Then there is a session from a different location, using a downgraded browser, but there was no transaction.

The location and browser information are suspicious enough to warrant closer monitoring of this account. Then there was a subsequent session with a high-value transaction, which clearly was suspicious, but was executed quickly enough that if the financial institution had not been on alert from the earlier activity, they might have missed it.

Business Banking

The established normal behavior included a single user, with the same computer, same IP address, consistent time of day, and a similar set of activities. What turned out to be fraud unfolded as follows:

1. The legitimate user (same computer, IP address, time of day) attempts to increase her own approval limit, but it doesn't work.
2. Then the user creates a new user and gives that person authority to approve very high value transactions. But there are no transactions attempted yet.
3. On a subsequent session, the user submits a wire transfer request.
4. Then the newly created user logs in for the first time and approves the wire.

This example turned out to be a Man-In-the-Browser attack in which the fraudster took over the victim's online session. The key clue here is adding a new user with a high approval level. Modifying the account profile like this frequently is cause for further investigation.

Business Practices for Banking Operations

The final best practices are business practices that guide how the financial institution responds to fraud when it does happen. Often this is what ultimately determines success or failure in preventing fraud.

Establish open internal communications channels – This is especially important across banking channels. Fraudsters are known to gather information online and then, for example, call customer service to request wire transfers using the information previously gathered.

- Include all departments: online banking, mobile banking, customer service, branch operations, back office, etc.
- Ensure everyone knows how to report suspicious activity to other departments and how to check with others.

Use case management and case documentation tools – Use these to track attacks, how each was resolved, losses, prevented losses, and other details. The information captured serves as an audit trail and helps to justify investments in fraud prevention technologies or services.

- Create a case for every suspicious session, summarize actions taken, and document the case resolution.
- Be sure to close the case to ensure accurate reporting of the number of cases that have been successfully managed.
- Use case management tools in conjunction with established policies, and be sure to follow internal processes and procedures for taking action and reporting on potential fraud incidents.

Be ready to move quickly – Fraud moves quickly. Fraudsters have the credentials, they've completed their reconnaissance and setup, and criminals often know the target institution's procedures ahead of time. When they strike, they move fast to get the transfer completed as quickly as possible before someone discovers what is going on and attempts to stop it (reinforcing the importance of being able to detect account takeover, reconnaissance and fraud setup well before a transaction has been initiated). Part of a financial institution's ability to move quickly is having procedures in place ahead of time rather than waiting for fraud to happen and then trying to quickly figure out how to respond.

Follow an established incident response process – Incident response typically includes: 1) Plan; 2) Detect and analyze what happened; 3) Contain the attack, eradicate the original source, and recover; and 4) Review all activity and update policies and procedures as appropriate.

Customer interactions – Effective customer interactions start with a focus on how to protect account holders, not just "stop fraudulent transactions." A financial institution should first ask, 'what is everything that can be done to protect the customer?' From educating customers about fraud to looking for compromised accounts to contacting customers if something suspicious arises, does the FI have processes in place to reach out to clients proactively in a timely manner?

Many institutions assume that contacting a customer about a suspected fraud incident will make the account holder upset or will create a negative impression of the institution. In fact, the opposite is true. Account holders are generally appreciative of outreach and of knowing that their FI is actively watching out for and working to protect their assets.

The key to successful customer interaction in the face of possible fraud is preparation.

- Be prepared with all of the information that may be needed about what has happened. This instills confidence in the client.

- Have a policy in place for how to communicate with the account holder depending on the severity or urgency of the situation. When to email vs. call, or when to call a second or third contact if the first is not available.
- Avoid alarming the client; communicate that the issue is under control. Have a script for the initial part of the conversation or a template for the email that demonstrates control over the situation and clearly communicates the situation and a recommended course of action.
- Know what options are available for responding to the suspicious activity, such as hold the transaction, put an alert on the account, or reset credentials. It is critical to have a clear recommendation that is appropriate for the risk level associated with each type of situation.
- Fraudsters have proven their ability to change the phone number on file with an institution and therefore be the person who is called to confirm the observed activity. To guard against this, the institution might include some red herring or out-of-wallet questions that could trip up the fraudster.

Align business objectives, company philosophy, and fraud policies – There is an inherent conflict between optimizing security and delivering great customer service. The customer service department will want to make it easier for customers to conduct business, which leaves the financial institution at greater risk for fraud. However, very tight security procedures that minimize the risk of fraud will make it harder on customers.

Establish priorities and communicate them to everyone internally so that all departments are working towards the same goal and clearly understand the tradeoffs. For example, if there is no transaction but just suspicious online activity, an institution may choose to lean more towards the best possible customer service and slightly lowered security policies (while staying alert and vigilant). But, if there is a potentially fraudulent transaction in question, then the institution may be more willing to sacrifice customer service for heightened security.

Know how fraud happens, how fraudsters operate – Understanding how fraud happens, how it works, the various schemes being utilized, and how fraudsters attack will result in being better prepared to recognize, detect, and defend against fraud.

- Subscribe to and monitor fraud alert services to stay abreast of new schemes or increased fraud activity levels.
- When rolling out new services, know how fraud can happen and what risks are introduced by the new service. This is part of a risk assessment called for by the FFIEC whenever a financial institution offers a new service or capability that introduces new risks.
- Train new employees and schedule regular continuing education to keep all employees informed about fraud, how it works, how to detect it, and established communications and response policies and procedures.
- Network with peers and fraud experts. Develop a community of fraud analysts by whom to run new threats, schemes, or response ideas, and with whom to share fraud experiences. The banking community must improve its ability to work together, sharing discoveries, warning each other, and working cooperatively to identify new attacks before they can be fully carried out or escalated.

ANOMALY DETECTION

Many of the best practices described in this paper rely on the ability to monitor and model many details regarding account holder behavior and then detect activity that is unusual or suspicious when compared to what is typical for each client. This capability is provided by a specific, more advanced application of anomaly detection called "behavior-based anomaly detection," and existing solutions are readily available for the banking industry.

Anomaly detection is the process of identifying anything unusual relative to something expected, i.e. detecting anomalies. Some anomaly detection solutions use aggregate, average, or population level data to indicate what is "normal." Behavior-based anomaly detection, on the other hand, looks at the unique behavior or each account holder.

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.

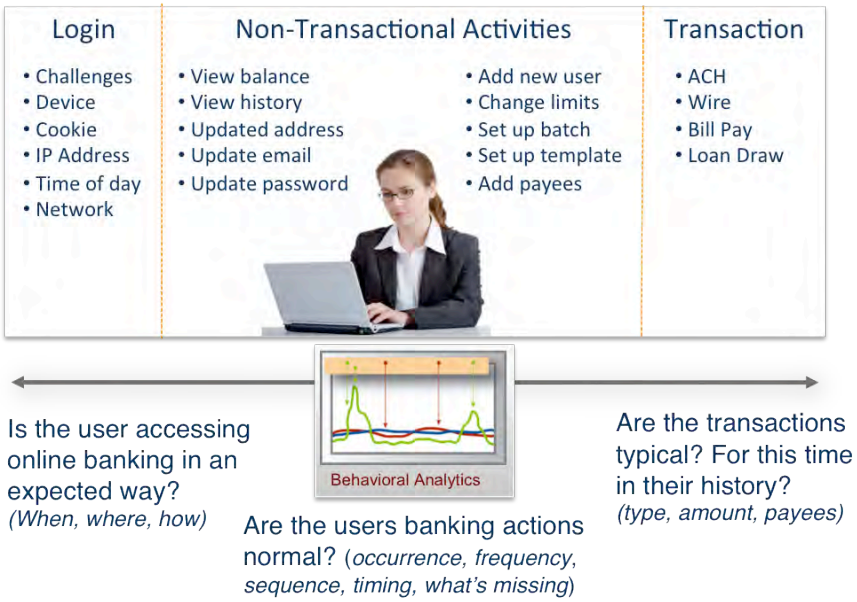


Figure 2: *Behavior-based anomaly detection solutions monitor all online and mobile banking activity, from login to logout.*

Examples of what behavior-based anomaly detection solutions can identify include the following (also see Figure 2 for additional examples):

- Accessing online banking from an unusual location or at an usual time of day
- Using online banking features not typically used
- Using online banking features in an unexpected sequence
- Changing account and profile information
- Adding payees
- Adding approvers or changing approval limits
- Submitting new types of transactions for unusual amounts or to new recipients
- An activity that is typically present in online sessions that now is omitted

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

One of the inherent benefits of using anomaly detection is that it can detect fraud regardless of what malware or fraud scheme is in play. It does not use 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.

To learn more, please download our **Practical Guide to Anomaly Detection**.

Conclusion

Cyber criminals spend every day developing new techniques and new technologies for stealing money. Preventing fraud requires adopting best practices that have been developed and proven in waging the day-to-day battles against the fraudsters.

Simply put, these best practices include being proactive, watching all activity from login to logout – not just the device, the login, or the transaction – and using individual account holder behavior as the best indicator of what is legitimate activity and what is suspicious and therefore requires additional investigation by the financial institution.

Behavior-based anomaly detection solutions model each individual account holder's behavior and look for unexpected activity that could be indicative of account takeover and fraud. By focusing on behavior instead of malware or specific attack schemes, anomaly detection solutions can detect new threats immediately without having to update rules, software, or malware profiles.

About Guardian Analytics

Guardian Analytics was founded in 2005 and is focused exclusively on fraud protection for financial institutions. We're proud to serve banks and credit unions that are taking a proactive approach to fraud prevention. Our customers take the promise of security very seriously – it's an essential element to protecting and maintaining their brands, their reputations, and their commitment to protect their institutions and their account holders from fraud attacks.

Our flagship solution, FraudMAP, is a behavior-based anomaly detection solution that was developed by leveraging our employees' direct experience and deep expertise in electronic fraud prevention – including solving actual fraud cases – built up over many years with extensive investment in intellectual property. FraudMAP is protecting hundreds of financial institutions of all sizes and millions of their account holders.

www.guardiananalytics.com