Bottomline™

Securing Digital Banking: Evolving Threats and Innovative Solutions

The Ongoing Evolution of Digital Payment Fraud

Payment fraud typology is constantly evolving – which is bad news for digital banking. Security measures that have traditionally served as effective protection are now being circumvented. Fraudsters are increasingly impersonating legitimate users, leveraging standalone or disconnected defense systems, and moving their attacks earlier in the payment journey.

The consequences of fraud sophistication are severe. A report from BAI shows that digital payment fraud losses are expected to surpass $343 billion globally between 2023 and 2027. Another recent study found that bad actors have stolen or compromised the personal information of 4 in 10 individuals in the past year. Fifty-one percent of these victims lost personal funds when fraudsters compromised their accounts, and half said these bad actors had targeted them more than once. On the corporate level, businesses average a loss of $200,000 per successful fraud attempt.

Relying on what has worked in the past will not secure digital banking in the present and the future. Understanding how payment fraud is changing will equip you to layer in critical security that will protect you from fraud – and from the negative customer experience, loss of reputation, and impact on your balance sheet that goes with it.

3 Dangerously Creative Threat Vectors

Creativity is a tremendous asset to getting a job done and done well. Unfortunately, fraudsters score high in creativity. Consider the following three threat vectors that involve fresh, innovative forms of payment fraud.

Sophisticated social engineering is a key component of most fraud attacks, including those discussed here. Social engineering can take the form of impersonating legitimate users, developing trust, mimicking a vendor or client, telling a convincing story, generating a sense of urgency, and more.

#1. Evolving Payment Rails

Payment rails continue to transform the digital payment landscape. These include The Clearing House Real-Time Payments (RTP) network, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the single euro payments area (SEPA) framework in Europe, and the FedNow payment rail that went live in 2023.

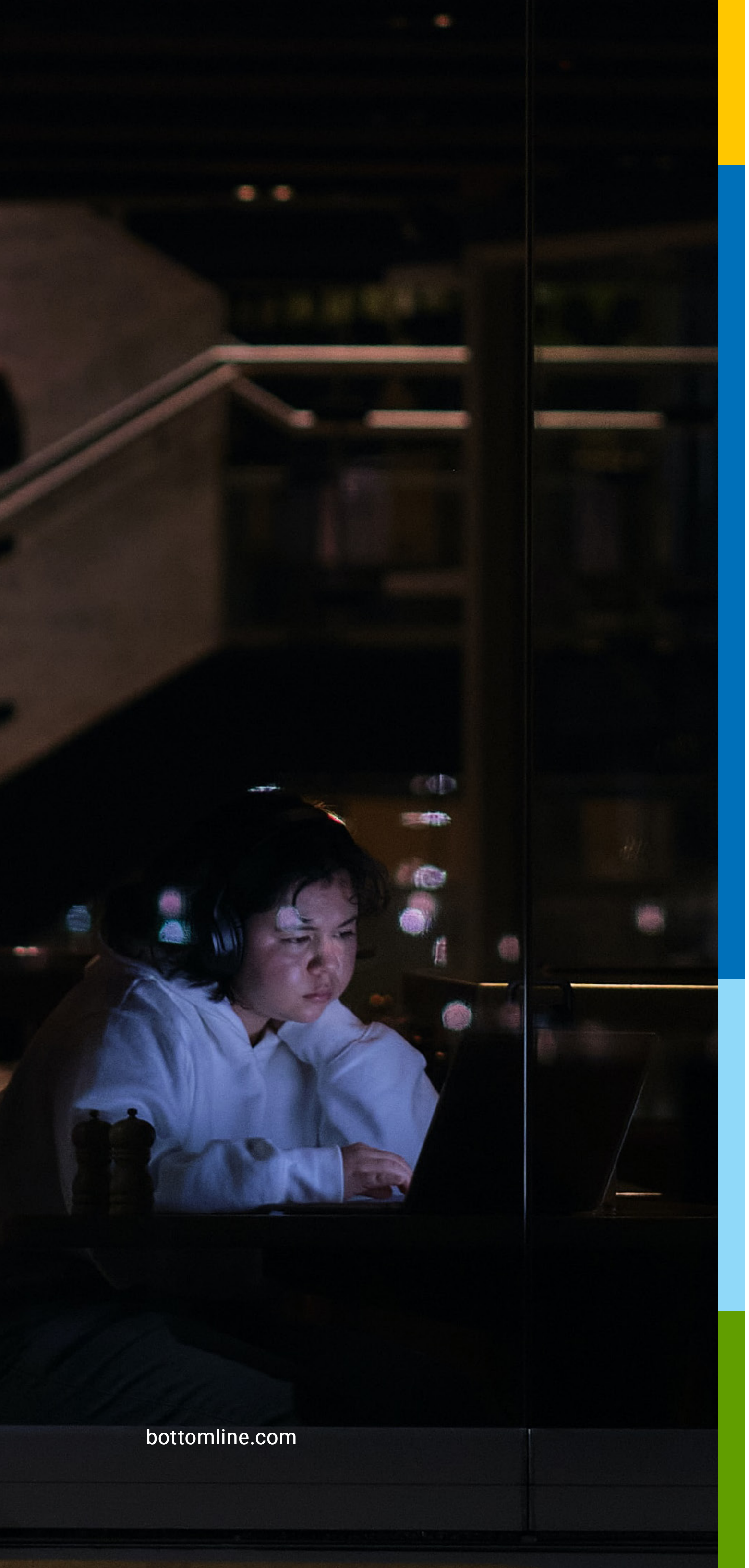
As payment rails evolve, so do the associated fraud opportunities. For example, The Clearing House (TCH) enables payors and payees to chat with one another. A fraudster can impersonate a payee, such as a vendor, and request payment for a (fake) invoice to be deposited into a specified account. If the fraudster has done his homework to make the request sound legitimate, the payor sets up an RTP. As simple as that, the fraudster has a fatter bank account with an instant, non-reversible, non-recoverable payment.

#2. Artificial Intelligence (AI) and Machine Learning (ML)

It is a truism that the more powerful something is in its potential for good, it is equally powerful in its potential for evil. Apply that to AI and ML, and it is understandable if you get shivers up your spine.

Consider deepfakes. Audio and video deepfakes are everywhere and are used in attacks on banks, businesses, and the person on the street. The average user, according to BAI, receives approximately 8 to 10 fake chatbot requests a week. It takes less than three seconds of audio for AI to mimic a person's voice. Therefore, even if a payor makes a call to confirm the legitimacy of a payment request, they could be talking to – and receiving assurances from – a robot and be none the wiser.

Then there are the evil cousins of ChatGPT: WormGPT and FraudGPT. WormGPT will answer questions about illegal activities, such as how to code malware or how to write a phishing email from a supposed CEO. FraudGPT is skilled at writing malicious code, finding vulnerabilities, and creating phishing pages, among other nefarious activities. As large language models are used more and more by solo hackers and crime organizations, the speed at which new frauds can be perpetrated will only increase – as will the "quality" of those fraud attempts.



#3. Website Impersonation

A third threat vector plaguing banks is website impersonation fraud, in which fraudsters create a duplicate of a legitimate website, such as that of a bank or business. AI often facilitates the swift creation of these duplicate sites.

A consumer or authorized business account administrator is then asked via digital ad, text message, or email to sign on to their account at this website. A link to the duplicate site is provided. The message looks completely legitimate and the website appears to be authentic.

Once on the duplicate site, legitimate users are tricked into providing their credentials, including the information needed to pass multi-factor authentication (MFA) challenges. This enables fraudsters to take over their account. The fraudster uses the credentials to transfer funds, access critical data, or both.

Identifying Gaps in Traditional Fraud Prevention

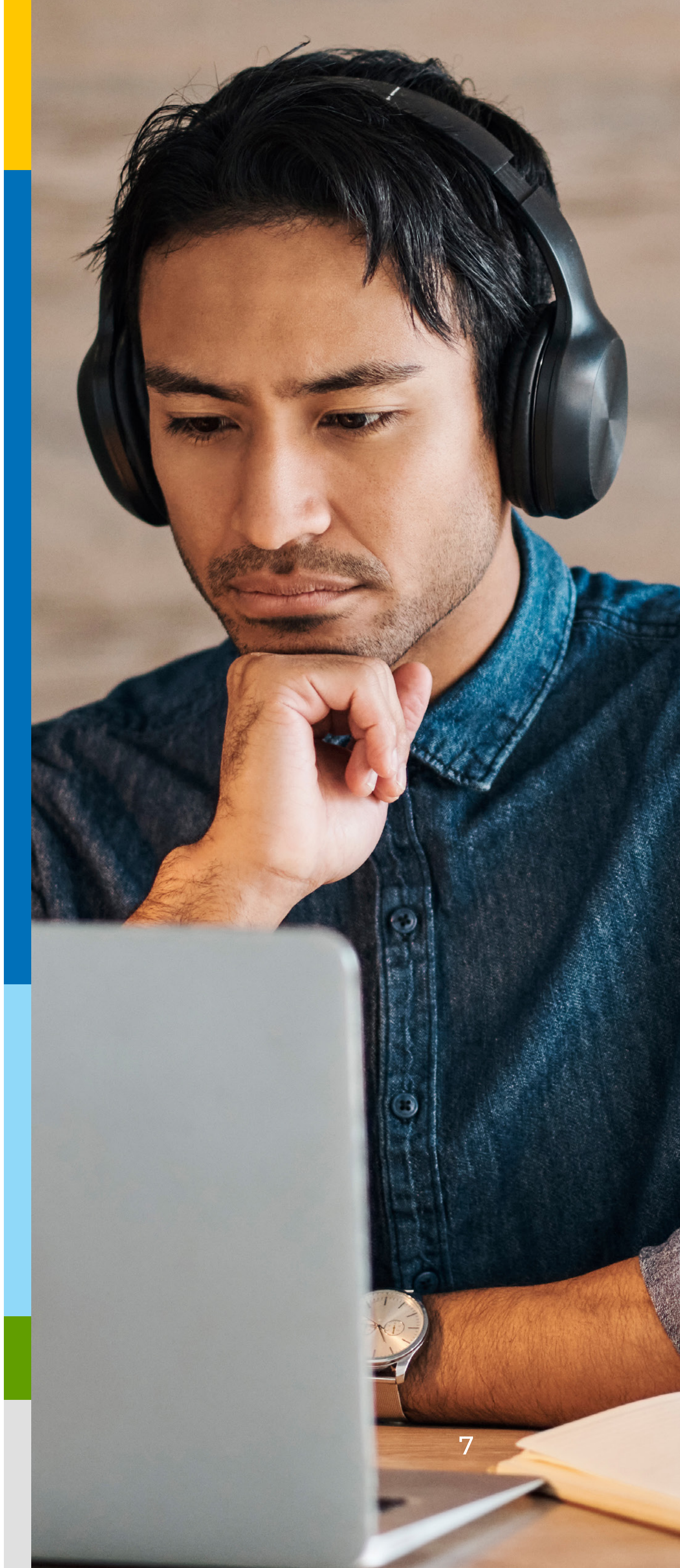
The following scenario – a composite of multiple real-world situations – shows how these threat vectors can be combined to accomplish digital payment fraud while evading traditional security measures.

Phase 1: Website Impersonation

A small but formidable crime ring conspires to target a bank. The team creates a precise replica of the bank's website, employing advanced AI/ML algorithms to enhance its authenticity. The cloned website includes a login page that closely mimics the original, making it virtually indistinguishable to unsuspecting users.

Phase 2: Digital Advertising

Once the false website is live, the group purchases ads on Google and other search engines. These ads appear to belong to the bank. The fraudsters know that when legitimate bank users search for the bank, some of them will click the link in one of the sponsored ads. Instead of being directed to the bank, however, the link will take the user to the duplicate login page.



Phase 3: Credential Harvesting

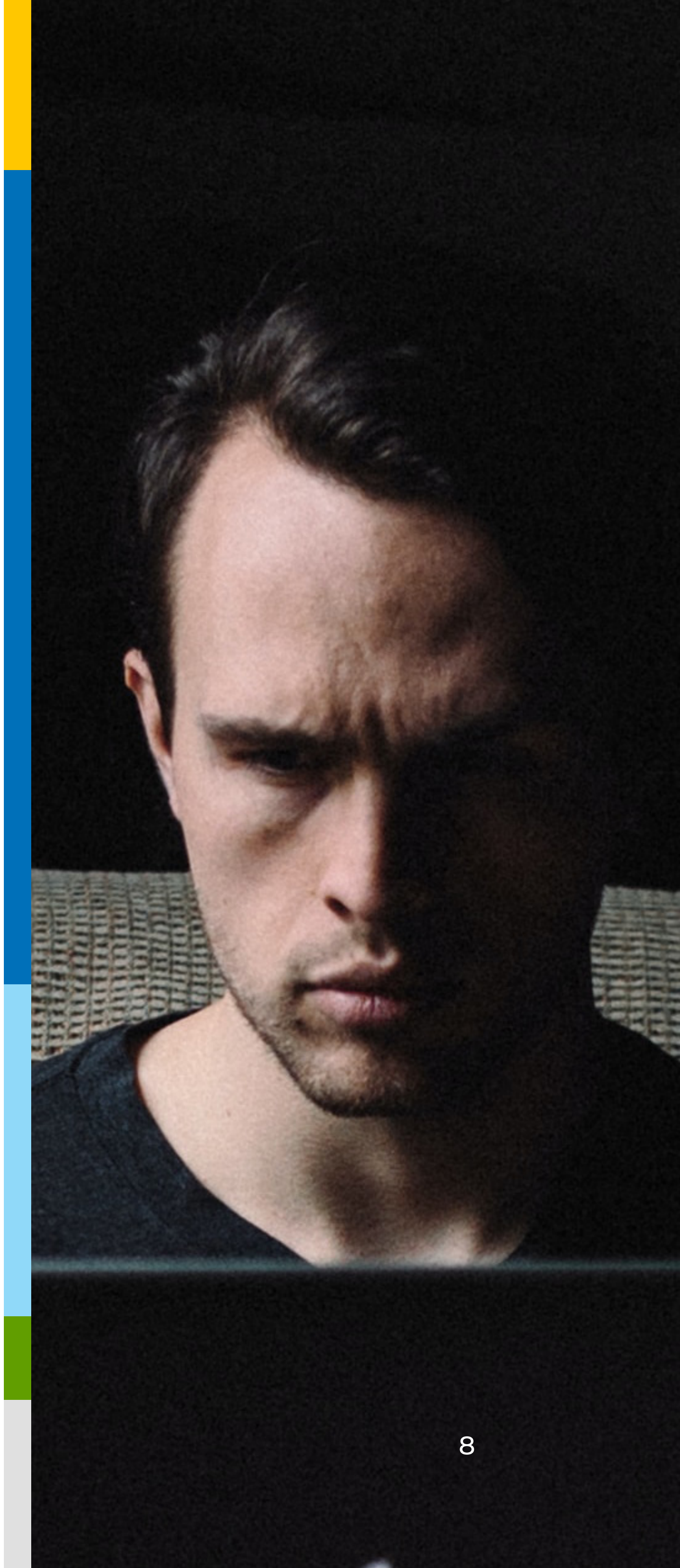
When a bank customer attempts to login on the fake portal (thus giving the fraudsters their username and password), they see an error message and a number to call for help. Pretending to be a helpdesk representative, one of the fraudsters builds rapport with the customer and manipulates them into revealing sensitive information, including the answers to their challenge questions.

Phase 4: Account Access

Having stolen customer credentials, fraudsters can answer MFA questions, get into customer accounts, and lay the groundwork for the eventual payment fraud. For instance, they may study customer habits, add payees, and modify account numbers. These non-monetary actions do not trigger alerts since the logins appear legitimate. And even if these actions trigger MFA challenges, which some payments systems can do, the fraudster has the information needed to move past them.

Phase 5: Real-Time Fraud

With a slew of compromised customer accounts, the crime ring leverages the FedNow payment rail to execute a set of real-time transactions. Because the fraudsters login with stolen credentials and schedule payments for amounts that match the customers' payment histories, they avoid detection by payment fraud monitoring systems. In a single night, they siphon off more than $1MM.



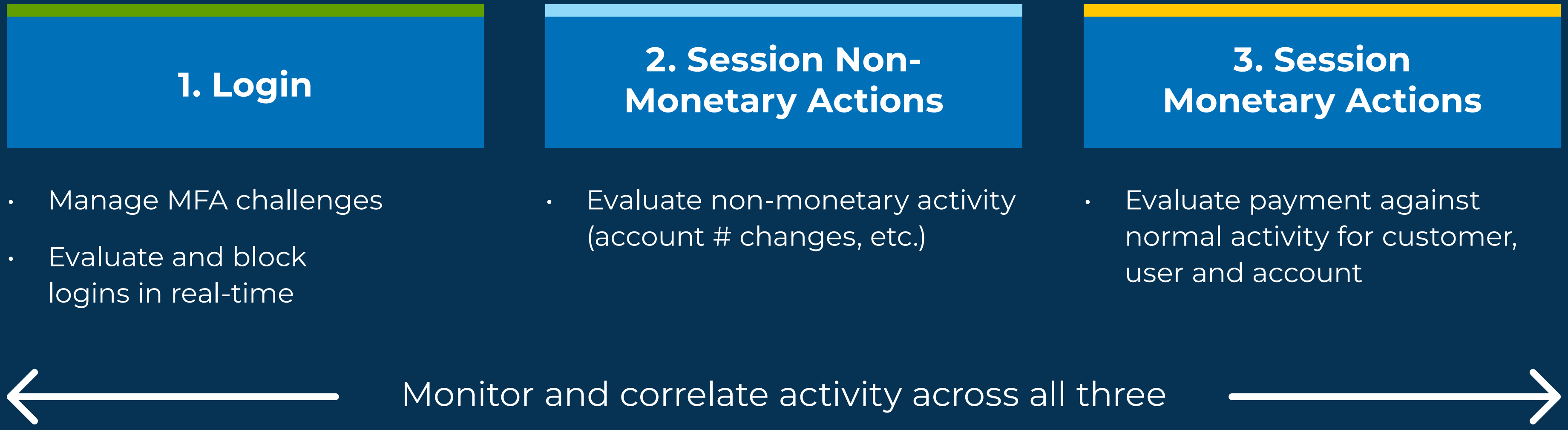
Connecting the Digital Banking User Journey

The scenario just outlined reveals the gaps left by traditional methods of fraud prevention. In particular, if banks rely upon disparate login, session activity, and payment monitoring tools, then fraudsters can find ways to avoid setting off alerts.

The good news is that banks can connect the full picture across the entire digital banking user session – from login through non-monetary actions to monetary transactions – through Bottomline's Secure Payments solution.

Secure Payments monitors the login, session, and payment activity of a customer to develop a detailed profile of what "normal" looks like for that user. Going forward, that profile is used to identify suspicious activity and implement real-time interdiction to place monetary transactions on hold pending investigation.

Digital Banking User Session



1. Login

- Manage MFA challenges
- Evaluate and block logins in real-time

2. Session Non-Monetary Actions

- Evaluate non-monetary activity (account # changes, etc.)

3. Session Monetary Actions

- Evaluate payment against normal activity for customer, user and account

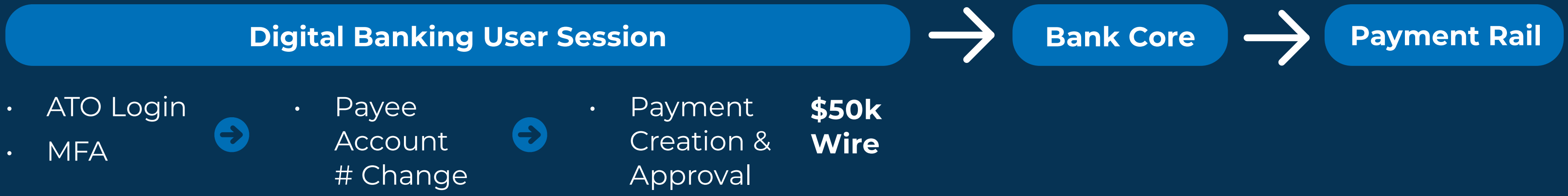
Monitor and correlate activity across all three

To illustrate the effectiveness of this approach, let’s take a closer look at a single transaction that was part of the scenario described earlier.

Disparate and Disconnected Tools Do Not Stop the Fraudulent Payment

Having hijacked a bank customer’s credentials, one of the crime ring logs in, complete with MFA, and takes a look at the customer’s account. He notes that it is a good target for the eventual heist, so he makes a change to a payee account number and logs off.

A week later, he creates and approves a wire transfer for $50K. The amount is typical, so it is unlikely an alert will be raised. Even if an alert is raised, the prior login and session activity are not factored into the evaluation of the payment. The payment goes through.



Digital Banking User Session → Bank Core → Payment Rail

- ATO Login
- MFA

→

- Payee Account # Change

→

- Payment Creation & Approval

$50k Wire

Fraud scenario likely won’t be stopped in time using downstream fraud monitoring alone

(Potential) Downstream Fraud Alert

- Evaluates payment, but $50k is normal payment amount and so are payments to new payees for this end-corporate
- Does not factor in prior login or session activity

Now, compare the same scenario to see what happens when Bottomline’s Secure Payments solution is in place.

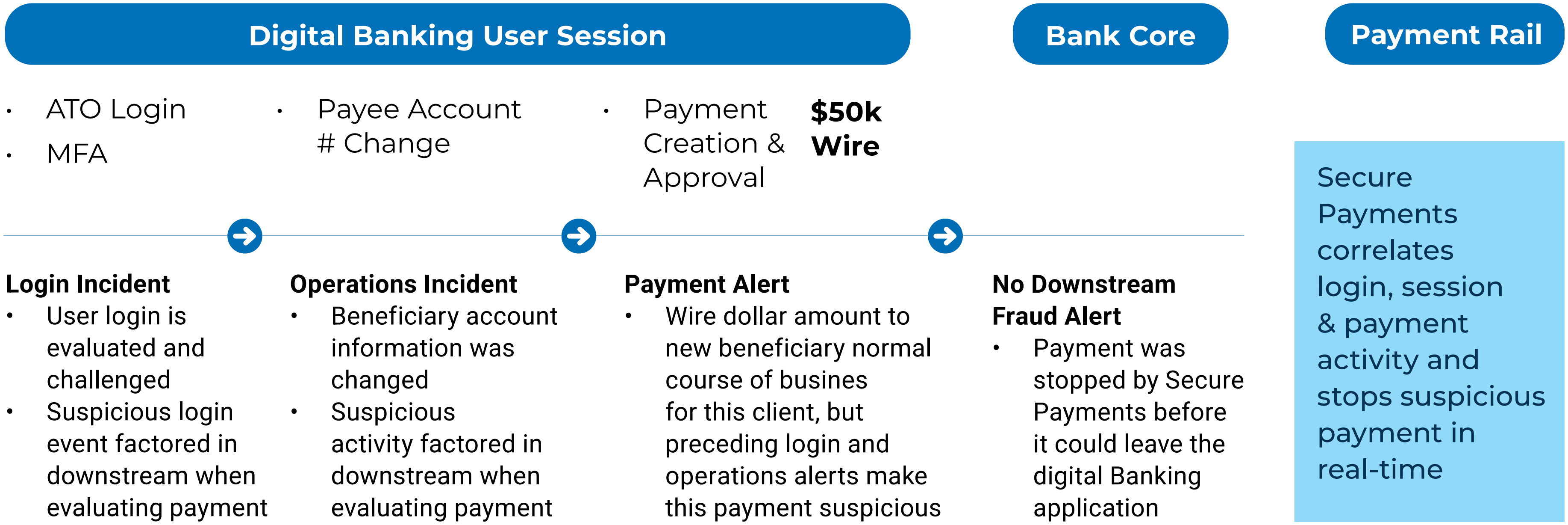
Connection and Correlation Stop the Fraudulent Payment

A member of the crime ring logs in with a customer’s stolen credentials. Secure Payments analyzes the login information, including time of day, IP address, and device fingerprint. Although the fraudster passes the MFA challenge, it is noted that the IP address and device fingerprint are not typical for the customer. Data about this suspicious login is retained for future reference.

The fraudster, noting that the customer is a good target, makes a change to a payee account number and logs off. Although this is a non-monetary event, it is also noted as being unusual customer session activity.

A week later, the fraudster logs in again and sets up a wire transfer for $50K.

The amount is typical, but Secure Payments factors in the previous suspicious activity and stops payment pending investigation. The Investigation Center is able to easily connect the dots across multiple logins, sessions, activities, and transactions to see what has transpired.



Digital Banking User Session

Bank Core

Payment Rail

- ATO Login
- MFA

- Payee Account # Change

- Payment Creation & Approval

$50k Wire

Login Incident
- User login is evaluated and challenged
- Suspicious login event factored in downstream when evaluating payment

Operations Incident
- Beneficiary account information was changed
- Suspicious activity factored in downstream when evaluating payment

Payment Alert
- Wire dollar amount to new beneficiary normal course of busines for this client, but preceding login and operations alerts make this payment suspicious

No Downstream Fraud Alert
- Payment was stopped by Secure Payments before it could leave the digital Banking application

Secure Payments correlates login, session & payment activity and stops suspicious payment in real-time

Investing in Enhanced Security

Bottomline's Secure Payments is completely customizable and configurable for each bank's needs and situation. For instance, alert thresholds can be set to certain dollar amounts or criticality levels. In that way, investigative resources can be allocated wisely to maximize effectiveness and productivity.

Additionally, the solution can be augmented with optional components and tools, including:

BTune:

Bottomline expert fraud and financial crime analysts work directly with banks to tune our fraud and financial crime solutions to their unique risk tolerance so customers only see the most meaningful alerts without missing out on suspicious activity.

FAST (Fraud Analytics Simulation Tool):

FAST helps banks compare risk models by enabling them to preview how changes in analytics settings will impact investigator workload, alert volume, and alert quality based on actual historical transactions.

BOLT (Bridge Over Lake Technology):

BOLT provides cloud data access to view, explore, analyze, export, and report on data above and beyond what can be done via the Secure Payments Investigation Center UI.

Intelligence Augmentation:

Secure Payments analytics can be amplified by ingesting intelligence from third-party providers to increase alert quality and reduce false positives. This capability eliminates the need to investigate alerts in multiple systems.

Record & Replay:

The Record & Replay tool captures both what a user sees and what a user does in the Commercial Digital Banking application. User sessions can then be visually replayed screen by screen, facilitating the investigation of suspicious activity.

Link Analysis:

Link analysis supports and streamlines investigations by creating a visualization of the relationships between various entities or activities.

Innovation and Optimization to Keep Ahead of Threats

At Bottomline, our primary goal is to make payments both streamlined and secure. Secure Payments, with its ability to provide a holistic picture of the digital banking journey and stop fraudsters in their tracks, is a vital part of our platform.

To that end, we invest heavily in optimizing and future-proofing Secure Payments. The user interface, detection and analytics features, integration capabilities, and performance standards are constantly being improved and enhanced. We are determined to stay on the cutting edge of technology and ahead of crime so you can focus on your business.

Learn more

Bottomline™

REV US082725LM