BANKING FRAUD DETECTION WITH DTEX

How Dtex helps global financial institutions detect bank fraud in the face of innovations in banking technology.

NEW TECHNOLOGY INNOVATIONS ARE FORCING FINANCIAL INSTITUTIONS TO RE-EVALUATE FRAUD DETECTION. **DTEX CAN HELP.**

Globally, financial institutions are learning how to adapt to the use of new, faster technology. A prime example is the New Payments Platform. The New Payments Platform (NPP) is a new, world-leading domestic payments infrastructure that enables connected Australian financial institutions to offer their customers – consumers, businesses and government agencies – near real-time, data-rich inter-bank payments at all times. The platform launched on 13 February 2018.

While the NPP and other technology advancements will enable a significant step forward in payment processing, this new platform also means that cyber-security tools must be held to a higher standard. Global financial organizations are revisiting their tools and frameworks, especially around the detection of bank fraud. The Dtex User Behavior Intelligence Platform can fill this gap.

REAL-TIME SYSTEMS & BANK FRAUD

For any financial institution, the potential for internal or external fraud is an operational risk present in all payment systems. This risk is more pronounced, however, in real-time payment systems because payment processing is so fast, as well as the typically irrevocable nature of real-time payments. Though real-time payment systems like NPP do not create new types of fraud, the velocity of payment processing does challenge financial institutions' existing fraud detection and prevention tools, since these solutions were designed for slower intraday and overnight batch processes.

To meet this challenge, institutions using real-time systems need to use a fraud risk management framework that focuses on identity, authentication and payment monitoring in real-time. Thus, participating financial institutions need to recognize the particular operational risks of processing velocity and 24/7 operations – including the need for effective real-time technology-based tools to manage banking fraud risks and protect their customers.

DTEX DETECTION

The Dtex User Behavior Intelligence Platform was purpose built to provide high-fidelity insights into user and identity behavior in real-time, and, as a result, enables organizations to effectively manage internal banking frauds. Banking fraud, or unauthorized transactions, occur if a customer's account is compromised and transactions are made without the customer's knowledge. Banking frauds can be classified as internal or external depending on where it originates (internal or external to the bank). In some cases, when there are external attacks that result in compromised machines, both can apply. This discussion will primarily focus on internal bank fraud, since Dtex was built to detect insider threats – including threats from malicious insiders, negligent insiders, and compromised machines (or credential theft). In the following pages, we will explore how Dtex can detect a variety of critical insider fraud use cases.

INTERNAL FRAUD USE CASE	DTEX DETECTION
Authentication & Access Behavior The first step to detect any insider bank fraud is to prioritize security authentication controls for local online banking infrastructure, including NPP infrastructure.	By deploying Dtex collectors on the local payments infrastructure – including endpoints, Jump Servers and Payment (NPP) Servers – institutions can detect which users and endpoints are logging into the local payment infrastructure. Any unusual access, unusual applications being used or deployed, unusual files being created or deleted can be detected by the Dtex anomaly detection algorithm.
Privileged Account Control and Logical Access Control Restrict and control the allocation and usage of administrator-level system accounts. Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.	Dtex provides visibility into the number of administrative/privileged accounts and how those accounts are used, as well as how privileges are shared. Dtex can alert on unauthorized sharing of privileges, shared administrative account use, and misuse of administrator accounts, ensuring that organizations can detect improper admin access.
Application Fraud (Using Identity Theft) Detect potential identity theft and understand how it occurred. Bank fraud can occur when machines in a bank are compromised or identities are stolen.	The forensic audit trail and the detection capabilities that Dtex provides mean that if a compromise does occur, Dtex can detect compromised machines and show organizations how that compromised actor interacted with company servers, endpoints, and data (including any payments infrastructure).
Data Security/Data Breach Ensure the security of the sensitive data that all financial institutions must protect, including personal information of all customers and other confidential data like credit card information. This data needs to be protected at all times.	Dtex collectors deployed in the organization monitor all highly sensitive data within an organization. This information is passed on to the analytics servers to baseline the user behavior on how the files are accessed, used, and deleted. These servers alert when they detect anomalies. They also capture data lineage, so that at any given point in time, there is always a record of how sensitive data moves and changes.
Phishing & Scams Organizations are vulnerable to targeted phishing with scam emails that prey on bank employees in order to gain credentials or steal personal information.	By looking at all website traffic and network traffic, Dtex can detect any new web/network anomalies when users click on phishing websites or visit websites with IP addresses that indicate risky websites.
Logging and Monitoring Record security events and detect anomalous actions and operations within the local environment.	Dtex collects user-focused metadata and combines that visibility with behavioral baselining, anomaly detection, and patterns of known-bad behavior to pinpoint risky user behavior. By deploying Dtex, organizations will obtain a high-fidelity insider threat signal.
Security Training and Awareness Ensure all staff are aware of and fulfill their security responsibilities by performing regular security training and awareness activities.	More than half of insider threat incidents are caused by negligence or human error, and Dtex was built with that in mind. It is impossible to effectively address the security mistakes happening within your enterprise without understanding exactly what those mistakes are. With Dtex's user behavior visibility, organizations are able to see the security mistakes that are putting data at risk, and customize their employee education accordingly.

In addition to the internal fraud use cases, Dtex can detect several external fraud use cases or supplement protection provided by other externally-focused security tools:

EXTERNAL FRAUD USE CASE	DTEX DETECTION
Automated User Account Takeover/Account Creation Recently, a wave of institutions have experienced automated attacks where armies of bots are used to crack username/passwords or are used to create new accounts to different websites. Fraudsters also are known to use hacking and phishing/social engineering scams to gain access to banking credentials.	By deploying Dtex on webservers, institutions can collect the incoming device & users details and understand abnormal activities, as well as alert on different attacks.
External Application Fraud (using Identity Theft). Application fraud involves using someone's identity to open bank accounts to procure credit cards/loans, steal money, or for use in other criminal activity.	There are two components to this use case: 1. Identity Theft: This was covered in the previous section under the "Application Fraud" use case. 2. As was shown in the previous use case, when accounts are created or accessed from unusual locations, Dtex can detect the anomalous network activity based on the incoming user information.
Hacking This involves exploiting security weaknesses on electronic devices or networks to commit identity theft and banking fraud. For example, hacking to gain access to banking credentials or modifying of an attribute (such as the account number or transaction amount) of a genuinely issued payment instruction.	Dtex detects when user accounts are accessed and alert when they are accessed at abnormal times. As Dtex does not look into the transaction content for privacy reasons, however, Dtex would not know the transaction amount or account number details.
Card Present Fraud Card present fraud involves fraudsters stealing a person's credit or debit card to make unauthorized purchases at point-of-sale devices, or to withdraw money via an ATM using a stolen PIN.	Though Dtex cannot detect directly whether a credit or debit card was stolen, when Dtex is deployed on the relevant payment servers, it can detect if any abnormal network activity occurs for a specific credit card. This would only be possible if profiling network activity by credit card.
Card Not Present 'Card not present' fraud occurs when debit or credit card details are stolen and used to make an unauthorized purchase or payment without the card, for example, online or by phone. Card not present fraud made up 78% of all fraud on Australian cards in 2016.	Though Dtex cannot detect directly whether a credit or debit card's details are stolen, when Dtex is deployed on the relevant payment servers, Dtex can detect if any abnormal network activity happens for a specific credit card. This would be only possible if profiling network activity by credit card.

Contact us today to find out more about how Dtex can help your financial institution protect against banking fraud:

EMAIL: info@dtexsystems.com | PHONE: +1 (408) 418 - 3786

References:
https://www.swift.com/myswift/customer-security-programme-csp/security-controls
https://assets.kpmg.com/content/dam/kpmg/au/pdf/2018/kpmg-nppa-new-payments-platform-minimising-payments-fraud.pdf