EXECUTIVE BRIEF
SEPTEMBER 2018

Preventing Banking Fraud and Breaches

How CA Technologies can help you

Privileged accounts and access are not just granted to employees with direct, hands-on responsibility for system and network administration but also vendors, contractors, business partners and others who use the systems within your organization. In many cases, privileged accounts aren't even people—they may be applications or configuration files empowered by hard-coded administrative credentials. In either case, they represent a target for external hackers or malicious insiders to compromise and exploit.

Background

Financial service organizations are under tremendous pressure to secure their financial, customer and other proprietary data against a burgeoning pantheon of internal and external threats. Whether access is gained maliciously or leveraged inappropriately by a valid user, exploited privileged user accounts are the common thread of most data breaches. The reality is that exploited or compromised privileged accounts are the cause for almost 50 percent of all data breaches,[1] regardless of whether those accounts were used by external actors with nefarious intent or simply abused by insiders. In fact, there are three primary challenges to banking organizations.

Challenge 1: Omnichannel Fraud Prevention

As the payments industry implements chips to reduce card-present fraud, card-not-present (CNP) fraud is increasing at an alarming rate. According to Statista, payment card losses due to counterfeit are expected to drop to $1.8 billion in 2018, a decrease of 60 percent from 2014. But Statista estimates that CNP fraud will increase to $6.4 billion in 2018, an increase of 220 percent since 2014.[2] According to Javelin Research, identity theft and fraud cost consumers more than $16 billion in 2017, and 81 percent of that was estimated to come from online transactions.[3] But account takeover also grew, tripling over the previous year to reach an all-time high of $5.1 billion. As banks seek to shore up their online payment security, they must also rethink how they are protecting their online banking applications.

A typical fraudster will purchase account and identity information on multiple users and multiple accounts on the Dark Net. If they attempt to complete a transaction on one channel, like an e-commerce transaction, and this fails, they simply go after the next channel or account associated with the same user. Without a cross-channel fraud prevention strategy and solution, the fraudster gains access to the online banking channel despite the fact that fraud was detected on the e-commerce channel. Cross-channel vulnerability is exacerbated by the number of accounts—credit and debit cards, online banking, mortgage, brokerage, etc.—that represent the way customers digitally interact with their financial institutions. In addition, if a fraudster is blocked from taking over a user's account, they just move on to the next user, either at the same bank or a different bank. Clearly, this type of attack requires a solution that tracks fraud across multiple financial entities.

Examples like this are causing a majority of companies to look toward innovative solutions that enable an omnichannel fraud prevention strategy—a strategy that involves maximizing the value of incoming transaction data to make intelligent real-time decisions on any given transaction, be it an e-commerce transaction, a wire transfer or an online banking login.

Challenge 2: Addressing Regulatory Compliance

In response to increasingly sophisticated electronic attacks against online banking and payments, numerous regulatory bodies and government entities have imposed mandatory controls and processes that banking institutions must implement to mitigate these risks. These include, but are not limited to:

- The Federal Financial Institutions Examination Council (FFIEC), which issued guidance that simple username/password was not sufficient for today's online banking environments
- The European Commission's second Payment Services Directive (PSD2), which imposes strong authentication requirements for banking and payment transactions and open and secure communications between banking entities
- The SWIFT Customer Security Controls Framework, which describes a set of mandatory and advisory security controls for SWIFT customers
- The Payment Card Industry Data Security Standard (PCI-DSS), which increases controls around cardholder data to reduce credit card fraud
- The 3-D Secure 2.0 protocol, which provides the ability to authenticate cardholders for online credit and debit card transactions, including in-app purchases, seamlessly across Web and mobile interfaces by providing access to data from the merchant and the card issuer

These regulations are just a few of the legal mandates with which banking institutions must comply, further underscoring the criticality of access control and auditing to prevent fraud and security incidents. Failure to comply can result in costly penalties and fines—and if data breaches do occur, the result can be lawsuits, damaged reputation and loss of constituent trust, as well as huge costs related to remediation of damages.

Challenge 3: Expanding Mobile Capabilities

Delivering native security along with a great user experience is critical to mobile banking and payments. Banking applications must provide greater assurance that users are who they claim to be. This is not only needed to guard against fraud, but also to build and maintain trust between banks and their customers. It also enables banks to leverage the convenience of the mobile platform to allow users to perform more sensitive transactions.

Challenge 4: Preventing Data Breaches

Although the number of reported breaches in the financial sector has fallen in the past two years, the banking industry continues to be a primary target for fraudsters. According to the 2018 Verizon Data Breach Investigations Report, the finance sector reported 598 incidents, which accounted for 7 percent of the reported data breaches. These attacks were carried out by both external actors (79 percent) and internal users (19 percent).

According to Ponemon, the average cost of each lost or stolen record is approximately $148,[4] and with most breaches involving millions of records, the costs of remediation are astronomically high. In fact, the average cost of a data breach is approximately $7.4 million.[3] But the threat extends beyond data breaches; fraudsters are also targeting ATMs to steal from banks and their clients. In fact, Kaspersky Lab reported that "an ATM-targeting malware called 'Cutlet Maker' was being sold openly on the dark net market for a few thousand dollars with a step-by-step user guide."[5]

What Organizations Must Do to Secure Access to Data

While the nature, extent and technological sophistication behind financial fraud and data breaches continues to evolve, financial institutions need to adopt a defense-in-depth strategy with multiple layers of security. In this new world, convenience and level of access is everything: How do you make doing business with your organization easy and convenient for customers while also ensuring the highest levels of security? Internally, which accounts have privileged access, what data they are accessing, and whether they need that level of access are critical elements to understand.

Many financial institutions are adopting strong authentication with user behavior models and analytics to address customer access and moving to what is known as a zero-trust model, in which all access is removed and then is granted back only when needed for internal users. For privileged accounts, this unique perspective requires organizations to control, manage and audit all privileged user access and activity. As part of this process, organizations are also looking to implement privileged identity governance, so that provisioning and de-provisioning of privileged access is automated, and additionally, periodic reviews and certification of this access are performed. The last thing financial institutions need is an angry ex-employee with the keys to the kingdom who walks out the door with proprietary data.

With this kind of access oversight and activity insight, financial institutions can combat insider threats as well as external attacks and secure their most precious asset: information. They can also address the two primary challenges discussed in the background section: preventing data breaches and addressing regulatory compliance.

Addressing Cross-Channel Fraud

To address cross-channel fraud, financial institutions must have a consolidated view of transactions across digital channels. Cross-channel fraud technologies can learn card, device, account, channel and user actions leveraging 3-D security and payment fraud data to detect and prevent fraud in real time, with deeper accuracy into the transaction's risk. This insight better enables organizations to seamlessly authenticate legitimate users and transactions while requiring strong authentication to those with a higher risk. Additionally, solutions that couple cross-channel fraud with a consistent authentication experience across channels are better able to not only detect and prevent fraud, but also to improve the overall user experience and reduce friction.

Implementing Controls that Auditors Are Seeking

Privileged access management technologies are not just good for combatting targeted breaches and insider threats; they can also help organizations meet regulatory requirements.[6]

Regulation Requirement	FFIEC	PCI	SWIFT	Comments
Identify and track the location of privileged account credentials	II.C.15	7.2.1	1.2	CA Privileged Access Manager (CA PAM) stores and manages privileged account credentials.
Enforce rules for password strength, uniqueness, change frequency	II.C.17	8.5.5 8.5.8 8.5.9	4.1	CA PAM automatically changes privileged passwords and enforces rules for strength and uniqueness.
Delegate so that only appropriate personnel have access	II.C.9 II.C.10(b) II.C.18	2.1 6.3.6 7.7.1 8.5.4 8.5.6	1.1 2.1 2.3 2.5 2.8 5.1	CA PAM only issues privileged access credentials to authorized users and can control what activities users can perform. In addition, CA Privileged Access Manager Server Control can harden any operating system.
Audit and alert to show requesters, access history, purpose, duration, etc.	III.B		6.4	CA PAM audits and can record all privileged account activity.

In addition, CA was the first vendor to successfully process EMV 3D Secure 2.0 transactions in production environments. We also provide solutions that address PSD2.

Deploying Mobile Banking Apps Quickly and Securely

CA Rapid App Security minimizes authentication and security friction for your customers by leveraging a transparent 2FA credential, a transparent contextual risk-based evaluation and an easy-to-use step-up authentication mechanism for high-risk transactions. The solution allows your developers to reduce the development cycle with frictionless and secure Web and mobile apps with one easy step that integrates device security and multi-factor and risk-based authentication. It provides users with fast and convenient access, helping the business strengthen consumer confidence. For mobile devices, it enables unequivocal trust between the user and the business by identifying the user, app and device and by learning and tracking the relationships between the three.

Preventing Data Breaches Before They Even Happen

To reduce risk, financial institutions must control the access of privileged users and track their actions. Privileged access management technologies focus on providing granular authorization of users to systems and accounts, auditing and recording attempts to access, and vaulting and rotating the privileged account's credentials, including passwords. In addition, when a privileged access management solution is integrated with user behavior analytics, organizations can detect risky activity and automatically trigger mitigations that limit the damage, which can be inflicted by a malicious insider or an external attacker leveraging a compromised privileged account.

Summary

To guard against costly data breaches, smart financial institutions are protecting and automating access to privileged accounts across both physical and virtual systems. Whether your company's data is on premises, in the cloud or within a hybrid infrastructure, it's critical to protect, monitor and audit privileged access everywhere. Employing a zero-trust model with a defense-in-depth approach to security that includes privileged access management offers your organization the best chance of protection against ever-evolving threats.

To learn more about privileged access management from CA, please visit **ca.com/privileged-access-management**

ca technologies

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

1 Verizon, "2018 Data Breach Investigations Report, April 2018, https://www.verizonenterprise.com/verizon-insights-lab/dbir/

2 Statista, "Value of payment card fraud losses in the United States from 2012 to 2018, by type (in billion U.S. dollars)," 2018, https://www.statista.com/statistics/419628/payment-card-fraud-losses-usa-by-type/

3 Al Pascual, Kyle Marchini, Sarah Miller, Javelin, "2018 Identity Fraud: Fraud Enters a New Era of Complexity," February 2018, https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity#

4 Ponemon Institute, "2018 Ponemon Cost of a Data Breach Report," July 2018, https://www.ibm.com/security/data-breach/

5 AO Kaspersky Lab, "Kaspersky Lab Bulletin: Threat Predictions for Financial Services and Fraud in 2018," November 2017, https://securelist.com/ksb-threat-predictions-for-financial-services-and-fraud-in-2018/83184/

6. Table Source: Barbara Filkins, "The Case for PIM/PAM in Today's Infosec," June 2016, https://www.sans.org/reading-room/whitepapers/analyst/case-pim-pam-todays-infosec-37072

Connect with CA Technologies

CS200-392392_0918