QUANTIFYING THE IMPACT OF CREDENTIAL STUFFING AND ACCOUNT TAKEOVERS IN FINANCIAL SERVICES

September 2021

Derek E. Brink, CISSP
Vice President and Research Fellow, Cybersecurity and IT GRC

ABERDEEN
STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

Executive Summary

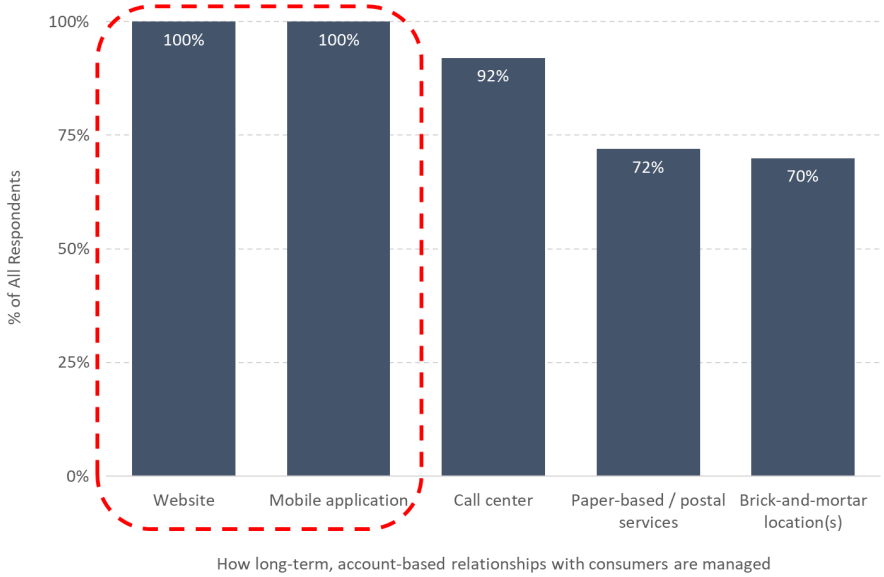
Financially motivated attackers have found *credential stuffing attacks* and *account takeovers* (ATOs) against organizations in the financial services industry to be a highly effective, highly scalable way to commit fraud. Aberdeen's quantitative analysis of the impact of successful ATOs demonstrates how the financial consequences have grown to a level that goes beyond a mere "cost of doing business," to become a material business risk — and provides insights into what's being done about it.

Attackers can access nearly 3.3B unique username / password pairs in the 1Q2021 "Compilation of Many Breaches" database.

From the perspective of financially motivated attackers, there are three obvious reasons why **credential stuffing attacks** against organizations in the financial services industry represent such a rich opportunity:

1. **Digital account-based relationships are based on digital user credentials, and credential stuffing attacks are an effective, brute-force way for attackers to exploit weak or compromised credentials and gain unauthorized access to user accounts.** Long-term, account-based customer relationships in the financial services industry are managed in a variety of ways — but in Aberdeen's recent research, *every* organization does so online, through both a website and a mobile application (see Figure 1).

Figure 1: Digital account-based relationships are based on digital user credentials, which are vulnerable to automated credential stuffing attacks.



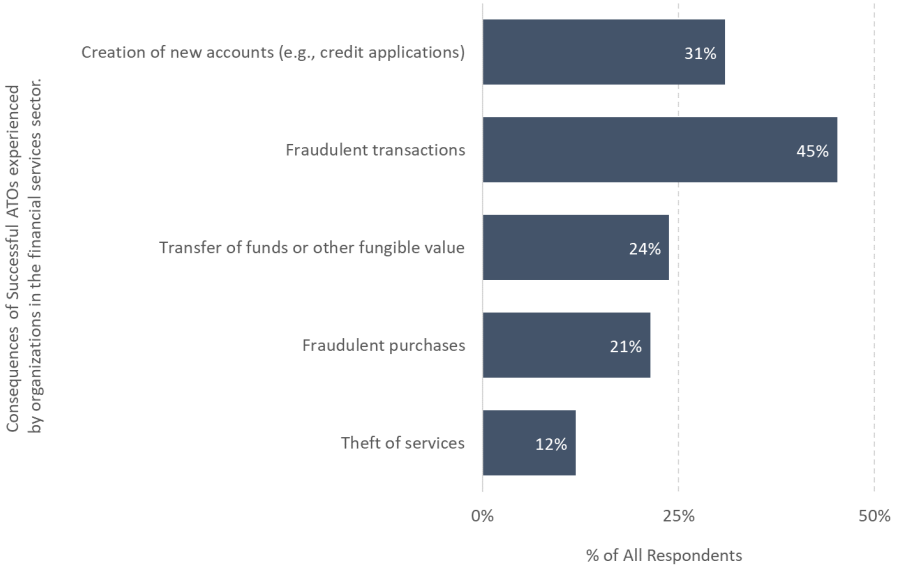
Source: Aberdeen, September 2021

- ***Credential stuffing*** refers to the process of automating the input of user credentials (e.g., obtained from a database of usernames and passwords that were compromised in a data breach, or obtained from a successful phishing attack) into the login page of a website or mobile app, in an attempt by an unauthorized party to achieve an ***account takeover***. Credential stuffing is commonly executed by ***bots***.
- ***Account takeovers (ATOs)*** refer to successful access to a legitimate user's account by an unauthorized party, as a means to commit financial fraud.
- ***Bots*** refer to small, purpose-built software programs that are designed to perform automated, repetitive, well-defined tasks — at Internet speed and scale.

2. **Credential stuffing attacks have become significantly easier for attackers to automate, at very large scale.** For their collective convenience, financially motivated attackers recently compiled and posted the user credentials derived from multiple mega-breaches (e.g., LinkedIn, Netflix, Gmail, Microsoft, Yahoo, Bitcoin) into a well-organized, searchable database of *nearly 3.3 billion unique username / password pairs*. The fact that so many of us continue to re-use the same passwords across our financial, eCommerce, social media, personal email, and work email accounts — combined with the fact that software **bots** are so brutally efficient at performing automated, repetitive, well-defined tasks at Internet speed and scale — has elevated bot-driven credential stuffing attacks to the top of the attacker's arsenal.

3. **Financially motivated attackers are making successful account takeovers pay off, in several ways.** As shown in Figure 2, Aberdeen's research found that organizations in the financial services industry experienced several direct consequences from successful ATOs, including *creation of new accounts* (e.g., credit applications); *fraudulent transactions*; *transfer of funds* or other fungible value (e.g., loyalty points, rewards); *fraudulent purchases* (e.g., physical goods, stored value cards); and *theft of services* (e.g., download or streaming of digital content).

Figure 2: Financially motivated attackers are making successful account takeovers in the financial services industry pay off, in several ways.



Source: Aberdeen, September 2021

By *quantifying* the impact of credential stuffing and account takeovers, Aberdeen aims to help organizations in the financial services industry make better-informed business decisions regarding what to do about this increasing risk.

From the defender's perspective, the flip side of the same three reasons discussed above are why organizations in the financial services industry are being forced to pay closer attention to credential stuffing and account takeovers:

- Digital credentials are central to the way they manage the long-term, account-based relationships with their digital customers.
- Bot-driven credential stuffing attacks are prevalent, and growing. In Aberdeen's recent research, **84%** of all respondents reported that some number of their online users had experienced a successful account takeover over the previous 12 months.
- The financial consequences of successful account takeovers — both direct, and indirect — have grown beyond a basic "cost of doing business" to become a material business risk.

84% of organizations in the financial services industry had online users who experienced a successful account takeover over the previous 12 months.

To help organizations make better-informed business decisions on this topic, Aberdeen conducted a benchmark study designed to *quantify* the **risk** (*how likely? how much impact?*) of credential stuffing and account takeovers for four segments of the financial services industry (Table 1).

Table 1: Aberdeen's benchmark study focused on four industry segments.

Segment	Description
Commercial Banks	Financial institutions that accept deposits, make various loans, and offer basic financial products like checking accounts, savings accounts, and certificates of deposit to individuals and small businesses.
Credit Unions	Not-for-profit financial institutions that are created, owned, and operated by their members, the individuals who deposit money into them.
Savings Institutions (S&L, Thrifts)	Banks that serve a local community by taking the deposits of local residents and lending the money back in the form of individual loans, residential mortgages, and small business loans.
FinTech	Innovative, tech-native services that aim to disrupt, compete with, and replace traditional approaches to the delivery of financial services, in categories such as *digital lending* (e.g., Kabbage), *mobile payments* (e.g., Venmo), *cryptocurrency exchanges* (e.g., Coinbase), *insurance* (e.g., Next Insurance, Lemonade), and *trading* (e.g., Robinhood, Webull).

Source: Aberdeen, September 2021

In its latest primary research project, Aberdeen focused on US-based organizations in each of these four segments that have online, account-based relationships with at least 50,000 monthly active users, and conducted phone-based interviews with individuals who had direct knowledge of key factors needed for a quantitative analysis, including:

- Number of Monthly Active Users (MAU)
- Monthly revenue per MAU
- % of MAU who experienced an ATO in the last 12 months
- Total cost of fraud from ATO (as a % of monthly revenue / MAU)
- Total annual cost of the people, tools (technologies), data, and services used to help the organization monitor and manage the negative consequences from successful ATOs to an acceptable level

A summary of the range of values for these factors is shown in Table 2.

Table 2: Primary research provided estimates for several key factors used in Aberdeen's quantitative analysis of the impact of credential stuffing and account takeovers in the financial services industry.

Factors Used for Quantitative Analysis of the Impact of ATOs	Commercial Banks	Credit Unions	Savings Institutions	FinTech
Revenue / MAU / month	$140 - $340 (median: $210)	$45 - $310 (median: $65)	$42 - $120 (median: $55)	$4 - $100 (median: $48)
Total cost of direct fraud from ATO (% of Revenue / MAU / month)	0.4% - 3.00% (median: 1.78%)	0% - 4.8% (median: 1.73%)	0% - 4.6% (median: 2.88%)	0% - 6.50% (median: 3.18%)
Total cost of monitoring and managing fraud from ATOs to an acceptable level ($ / MAU / month)	median: $1.80	median: $2.10	median: $2.10	median: $0.60
% of MAU experiencing an ATO as a result of a successful credential stuffing attack	0% - 1.70% (median: 0.85%)	0% - 1.50% (median: 0.60%)	0% - 4.60% (median: 0.80%)	0% - 1.50% (median: 0.58%)

Source: Aberdeen, September 2021

The **total cost of direct fraud from ATO** attacks represents the range of estimates from subject-matter experts in each segment for the consequences previously noted in Figure 2: creation of new accounts (e.g., credit applications); fraudulent transactions that result in chargebacks and false declines; transfer of funds or other fungible value;

fraudulent purchases; and theft of services. In addition, the subject-matter experts estimated the **total annual amount their organizations are investing in people, tools (technologies), and data** to help them manage the negative consequences from successful account takeover attacks to an acceptable level. Often, these costs also include escalating payments to service providers to build and tweak custom, ever-changing rules.

Taken together, Aberdeen's quantitative analysis estimates the **total annualized direct impact of fraud from account takeovers** for each of the four market segments, as a percentage of the revenue generated from monthly active users:

- Commercial Banks: Between **1.9% - 3.5% (median: 2.7%)**
- Credit Unions: Between **2.2% - 7.7% (median: 5.2%)**
- Savings Institutions: Between **4.4% - 8.3% (median: 6.4%)**
- FinTech: Between **2.6% - 7.1% (median: 4.8%)**

Separately, respondents in Aberdeen's study identified several **indirect costs resulting from account takeovers**, such as:

- Need for users to engage with a Call Center representative (e.g., for investigation and resolution of account status, help with password resets, and so on)
- Negative publicity / social media / online reviews
- Attrition in the total number of monthly active users because of security (i.e., users become less active); closure of accounts; loss of market share to competitors
- Data breach of account holder data (e.g., compromise of personally identifiable information, protected health information)
- Increased scrutiny from industry regulators

These too can be quantified. As an illustrative example, Aberdeen extended its Monte Carlo analysis to estimate the **impact of MAU attrition resulting from account takeovers**, also expressed as a percentage of the revenue generated from monthly active users. By definition, this estimate reflects an *understated*, *conservative* estimate of the total indirect costs from ATOs:

Taken together, the total cost of direct fraud from ATO attacks — combined with the total annual cost of people, technologies, data, and services to help manage it — have grown to a level that makes it a material business risk.

- Commercial Banks: Between **0.8% - 4.0% (median: 2.0%)**
- Credit Unions: Between **0.5% - 3.3% (median: 1.5%)**
- Savings Institutions: Between **0.2% - 8.4% (median: 2.7%)**
- FinTech: Between **0.5% - 3.2% (median: 1.5%)**

Aberdeen's estimates for direct and indirect impact from ATO for each segment is summarized in Table 3. This demonstrates the key insight, already mentioned above: The financial consequences of successful account takeovers have grown to a level that goes beyond a mere "cost of doing business," to become a material business risk.

Table 3: Aberdeen's quantitative analysis of the impact of credential stuffing and account takeovers in the financial services industry demonstrates that it has grown to become a material business risk.

Annualized Impact of Account Takeovers	Commercial Banks	Credit Unions	Savings Institutions	FinTech
Direct: The cost of fraud from ATOs, and the total cost of managing it	1.9% - 3.5% (median: 2.7%)	2.2% - 7.7% (median: 5.2%)	4.4% - 8.3% (median: 6.4%)	2.6% - 7.1% (median: 4.8%)
Indirect (illustrative): The impact of MAU attrition from ATOs	0.8% - 4.0% (median: 2.0%)	0.5% - 3.3% (median: 1.5%)	0.2% - 8.4% (median: 2.7%)	0.5% - 3.2% (median: 1.5%)

Source: Expressed as a percentage of the revenue generated from Monthly Active Users; Aberdeen, September 2021

Readers are encouraged to use these research-driven findings to make a quick, personalized estimate of the total annualized impact of credential stuffing and account takeovers for your own organization. For example:

- Segment: Commercial Banks
- Number of monthly active users: 100,000
- Revenue from monthly active users: $210 / month
- Annual revenue from MAU: (100,000) x ($210) x 12 = $252M
- Impact of ATOs (direct): $252M x (1.9%-3.5%) = $4.8M-$8.8M
- Impact of ATOs (indirect): $252M x (0.8%-4.0%) = $2.0M-$10.1M
- Total annualized impact of ATOs: **$6.8M-$18.9M / year**, or **2.7%-7.5% of annual revenue**

Financial services organizations are making incremental investments in security technologies designed to help address the issue of credential stuffing and ATOs — here's where.

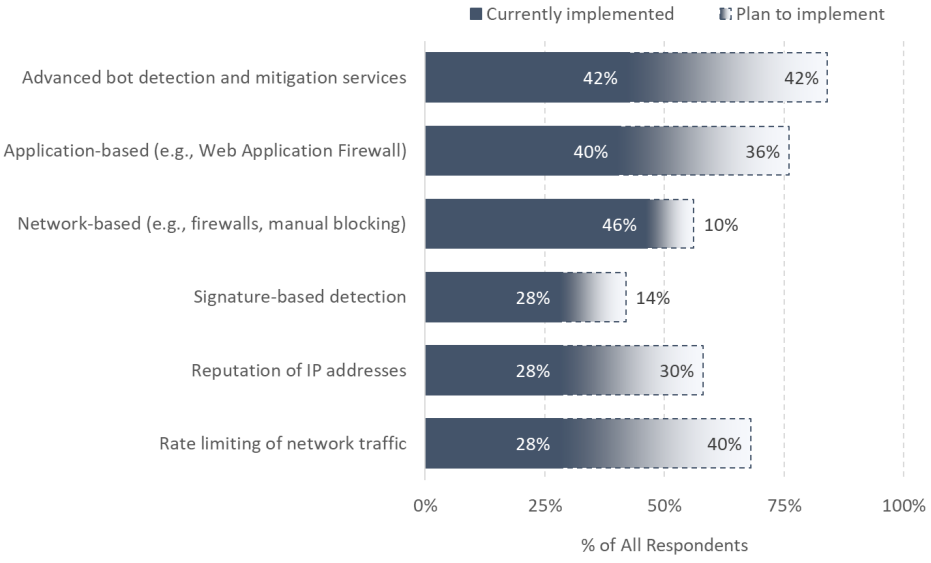
As part of its research project, Aberdeen also asked respondents to rank the key drivers behind the incremental investments they are making (or plan to make) to help address the growing issue of credential stuffing and account takeovers. In terms of high-level technology categories, here are the top two strategies:

- **Reduce the effectiveness of automated credential stuffing attacks** (e.g., adopt stronger bot detection and mitigation capabilities) — on average, representing 42% of the total point allocations.
- **Reduce the weaknesses of passwords and password re-use that lead to successful account takeovers** (e.g., adopt stronger user authentication capabilities) — on average, representing 14% of the total point allocations.

Said another way: To address the issue of credential stuffing and account takeovers, organizations in the financial services industry are about 3-times more likely to invest in fighting malicious bots than taking steps to reduce the weaknesses of passwords and password re-use.

To address the issue of credential stuffing and account takeovers, organizations in the financial services industry are about 3-times more likely to invest in *fighting malicious bots* than in taking steps to *reduce the weaknesses of passwords and password re-use*.

Figure 4: Advanced bot detection and mitigation services top the list of technical capabilities being adopted to reduce the effectiveness of automated credential stuffing attacks in financial services.



Source: Aberdeen, September 2021

To be clear, financial services organizations are actively investing in both of these areas — but arguably there are a much wider range of considerations for making changes to user authentication, which directly affects the daily experience for tens of thousands of online account holders.

In contrast, fighting malicious bots generally takes place behind the scenes, at the infrastructure level, which in Aberdeen's view makes the path to adoption and results more direct and less complicated.

As shown in Figure 4, **advanced bot detection and mitigation services** top the list of technical capabilities being adopted to reduce the effectiveness of automated credential stuffing attacks in the financial services industry, which in turn reduces the likelihood of successful account takeovers and the corresponding business impact.

***Advanced bot detection and mitigation services* top the list of technical capabilities being adopted to reduce the effectiveness of automated credential stuffing attacks in the financial services industry.**

Summary and Key Takeaways

- From the perspective of financially motivated attackers, there are three obvious reasons why **credential stuffing attacks** against organizations in the financial services industry represent such a rich opportunity:
  - Credential stuffing attacks are an effective, brute-force way for attackers to exploit weak or compromised digital credentials and gain unauthorized access to user accounts.
  - Credential stuffing attacks have become significantly easier for attackers to automate, at Internet speed and scale.
  - Financially motivated attackers are making successful account takeovers pay off, in several ways.
- From the defender's perspective, the flip side of these same three reasons are why organizations in the financial services industry are being forced to pay closer attention to credential stuffing and account takeovers:
  - Digital credentials are central to the way they manage the long-term, account-based relationships with their digital customers.

- Bot-driven credential stuffing attacks are prevalent, and growing.
- The financial consequences of successful account takeovers — both direct, and indirect — have grown beyond a basic “cost of doing business” to become a material business risk.

- To help organizations make better-informed business decisions on this topic, Aberdeen conducted a benchmark study designed to quantify the risk of credential stuffing and account takeovers for four segments of the financial services industry, as a percentage of revenue generated from monthly active users:
  - *Commercial Banks: Between 2.7% - 7.5% (median: 4.7%)*
  - *Credit Unions: Between 2.7% - 11.0% (median: 6.7%)*
  - *Savings Institutions: Between 4.6% - 16.7% (median: 9.1%)*
  - *FinTech: Between 3.1% - 10.3% (median: 6.3%)*
- The key takeaway: The financial consequences of successful account takeovers have grown to a level that goes beyond a mere “cost of doing business,” to become a material business risk.
- To address the issue of credential stuffing and account takeovers, organizations in the financial services industry are about 3-times more likely to invest in *fighting malicious bots* than in taking steps to *reduce the weaknesses of passwords and password re-use*.
- **Advanced bot detection and mitigation services** top the list of technical capabilities being adopted to reduce the effectiveness of automated credential stuffing in the financial services industry, which in turn reduces the likelihood of successful account takeovers and the corresponding business impact.

Related Research

- *Quantifying the Hidden Business Impact of Web Browser Extensions on eCommerce Merchants*; September 2020
- *The Business Impact of Website Scraping: It's Probably Bigger Than You Think — Here's Why*; May 2020
- *User Authentication for Online Services: Friction = Failure*; April 2021
- *Digital Enrollment in Financial Services: An Easy and Effective Starting Point*; August 2019

About Aberdeen Group

Since 1988, Aberdeen Group has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen Group is headquartered in Waltham, Massachusetts, USA.