FAQ
Credential Stuffing and Brute Force Login Attacks

What is a brute force login attack (BFA)?

A brute force attack is when a large number of login credentials are automatically entered into a website until they are potentially matched to an existing account to grant access, which the attacker can then hijack for their own purposes.

What is a credential stuffing attack (CSA)?

Credential stuffing is the automated injection of leaked username/password pairs in order to fraudulently gain access to user accounts. This is a type of brute force attack, where large numbers of login credentials are automatically entered into a website until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.

How big are these attacks?

Credential and brute force login attacks vary in size considerably. Some attacks are very small (only a few hundred attempts per hour) and are difficult to differentiate from normal activity, while others can be very large (millions of attempts per hour). Although larger attacks pose no threat to NCR's digital banking infrastructure, they often result in a large number of locked end user accounts. This in turn results in increased inbound phone traffic from end users to their financial institution.

What makes these attacks possible?

Large password lists consisting of leaked username/password combinations are made available on the Internet. These lists are often compiled from credentials stolen during large scale breaches of organizations such as LinkedIn, MySpace, Yahoo, Dropbox and others. While these companies have done their due diligence by asking their users to change their login credentials, password reuse remains a common issue. This allows threat actors to use compromised account credentials on other websites and services.

Additionally, threat actors take advantage of the fact that many end users reuse weak credentials. Credential-stealing malware is often employed by threat actors to harvest end user data.

Are brute force and credential stuffing attacks considered fraud?

Brute force and credential stuffing attacks fall into the category of suspicious login activity that could be associated with certain types of digital banking fraud, such as *account takeover*. While the two events could be connected, we've also seen instances where the activity is only coincidental; this is why we refer to these attacks as suspicious activity and not fraud. Ultimately, your financial institution makes the final determination of fraud.

Did this attack affect NCR's other financial institution customers?

While NCR only discusses the details of suspicious activities with the financial institution to whom they directly apply, we can say that these types of attacks are common and often include multiple websites as their targets. Beyond that, it's difficult to correlate the many symptoms of the attack due to the hundreds (if not thousands) of IPs utilized and the wide variety of devices often employed in a single attack.

What process does NCR have in place to respond to these attacks?

NCR proactively monitors for brute force attacks by analyzing bad login activity with both automated and human analysis to determine the scope and impact of such attacks:

1. **Identify the attack**
   a. We constantly monitor for brute force attacks through automated log processing and the NCR Security team also proactively monitors for activity that correspond to brute force attacks.
   b. Financial institutions also identify and report events based on data from their security monitors or after finding unusual activity (like locked accounts) through analysis of NCR Digital Banking reports.

2. **Escalate to Security**
   a. After an event is identified or reported, the security team runs a series of reports to gather key data and help determine any action items or mitigations.

3. **Evaluate and categorize the event**
   a. The event is categorized by the Security team based on size, user impact, and frequency or recurrence.
   b. A final impact determination is made based on the above and next steps are performed based on that determination.

4. **Contact the affected financial institution**
   a. The Escalations team will typically notify a financial institution of the event if needed (unless other arrangements have been made) and answer all of their questions.
   b. The financial institution is provided with a summary of the event and a list of actionable preventative measure options based on the situation.

When does NCR communicate these attacks to affected financial institutions? Is there a severity threshold for you to communicate to us?

Credential and brute force login attacks vary in size considerably and we are aware that some financial institution tools (such as Guardian Analytics) may auto-generate alerts in response to suspected BFA & CSA activity.

NCR, however, *does not* track and profile digital banking behavior at the individual end user account level as many of these other solutions do. Because of this, there is currently no preset, FI-specific "severity threshold" to communicate for brute force and credential stuffing attack activity. What may look suspicious for one financial institution may be business as usual for another on any given day.

NCR's digital banking Security Team, however, does maintain a set of indicators of suspicious activity and proactively monitors for these types of attacks by analyzing bad login activity.

What countermeasures does NCR currently have in place to reduce the risks from these attacks?

Brute force and credential stuffing attacks are increasing and there are a variety of tools we use to limit their impact.

NCR has implemented multi-factor authentication (MFA) to harden its authentication process. A common result of a credential stuffing attack is a *user name only* match occurs, which results in the user account being locked after several wrong password attempts are made. In the event that both the username and password are matched, multi-factor authentication will thwart the unauthorized account login as attackers do not have access to the secondary authentication method.

Time-based lock out protocols are also available to our financial institutions. This method allows a financial institution to force a time delay period (varying from seconds to hours) after successive login attempts fail. In some cases, the IP addresses from the attacking source may also be blocked. This countermeasure has very limited effectiveness, however, as the attacker will simply move to a different IP source.

While these types of attacks will evolve, user account lockout issues remain the most common issue impacting our financial institutions and end users today.

What can my financial institution do to help mitigate the risk from these attacks?

Since the threat actors have access to large lists of potential user login credentials, hardening both the user account credentials as well as the login process can provide *significant* deterrence to threat actors, thus reducing the possibility of account compromise form this type of attack.

User account credentials can be hardened by the following measures:

- Increasing password length and complexity (we recommend at least 12 characters including numbers, upper/lower case letters and special characters)
- Disallowing personal identifiable information to be used as login ID's, such as social security numbers and email addresses.
- Requiring password changes and enforcing a password no-reuse policy

Login process hardening can be accomplished by the following measures:

- Implementing multi-factor authentication (MFA) for user logins
- Implementing time-based lock out protocols where login delays are incrementally increased after a predefined number of bad login attempts

What else is NCR considering to help mitigate risk from these attacks?

Because security is essential, we continually invest in additional enhancements. Recent enhancements across the industry to mitigate BFAs are countermeasures, such as captcha, enhanced complex device identification (CDI) and others to address these types of threats.