Account Data Compromise
Best Practices for Issuers

The following best practices are intended to help issuers manage their fraud risk on accounts that have been exposed as part of a data compromise.

Before Identify | During Prevent | Ongoing/After Monitor & Recovery

Before: (Identify)

Issuers with processes in place to identify potential points of compromise should report any potential compromises to Visa for further investigation. Guidelines on the Common Point of Purchase (CPP) process may be found on the Visa Online site located at www.visaonline.com under the Risk tab, then "Fraud Risk Products and Solutions" and "Common Point of Purchase (CPP)"). Issuers that find potential points of compromise should gather all accounts for the suspected "at-risk" timeframe and begin to analyze patterns and test fraud mitigation rules. Issuers can also consider leveraging cyber intelligence available through their internal information security teams to understand whether compromised account data is being sold on the dark web or in underground markets.

During: (Prevent)

Once a compromise is identified, issuers should immediately monitor "at-risk" accounts. Therefore, upon notification, issuers should download accounts from the Compromised Account Management System (CAMS) as soon as possible. CAMS alerts are available exclusively through Visa Risk Manager, accessible through Visa Online. If you subscribe to this service, you will find it listed as "Visa Risk Manager" under "My Services" on the Visa Online home page. Access to Visa Risk Manager can be requested through the "Request Additional Services" link in the same section. Ideally, issuers should use the alert information, along with the accounts at risk, to utilize the risk-decision systems (e.g., Visa Risk Manager). Issuers may also use the Compromised Event Reference (CER) ID as a way to flag and/or identify the impacted accounts.

Issuers should check whether their processor allows for immediate account upload to its fraud management tool to queue and flag accounts for further action. Visa Debit Processing Services (DPS) has a free "on-behalf-of" service that issuers must "opt-in" to use.

From an authorization and customer service standpoint, it is important that accounts involved in a compromise are easily recognized. Flags for early fraud detection can help fraud managers create targeted mitigation strategies and controls. Flags also allow fraud operations and dispute teams to efficiently assess risk on an account and take proper action. If you offer alerts, encourage your customers to enroll in them. Keep call center scripts simple, and remind customers of zero liability—contact your Visa representative for more information. You can also explore implementing two-way, multi-channel fraud alerts as an effective method to confirm with the cardholder whether a transaction in question was legitimate. This is effective and available for both compromised and non-compromised accounts. Proactive alerts provided to cardholders can help issuers take immediate steps to address any potential fraudulent action on an account, reducing the fraud run and minimizing issuer loss.

Start to control potential fraud and tailor controls for the type of compromise

Issuers should align initial fraud controls with the type of data exposed—for example, track data with card-present fraud; account number/CVV2 with card-not-present (CNP) fraud. If the type of account data that may have been exposed is unknown, add general controls for all types of fraud. Be cautious not to over-control, however, to avoid a negative customer experience at the point of sale.

Once fraud begins to occur on compromised accounts, adjust fraud rules based on the type of fraud to minimize negative impacts on cardholders. Being surgical, minimizing impact on low risk transactions, and avoiding unnecessary actions that could cause disruptions at the point of sale will maintain customer satisfaction levels.

Note: Fraud controls can be online with real-time decline at the point of sale, or offline with less impact to authorizations. From a customer's perspective, it is better that the issuer detect fraud. Research shows this is a key factor in maintaining customer trust.

Ongoing/After: (Monitor & Recovery)

Watch for pattern changes tied to the compromise

Because fraud changes quickly, issuers should track patterns as they are reported to properly create or adapt fraud controls. For example, compromises that involve track data are expected to result in counterfeit fraud. Although the initial controls may be focused on card-present transactions, card-not-present fraud may occur as well. Watch for changing patterns and adjust rules as necessary.

Card Reissuance – Points to Consider

Reissuance of cards is expensive to issuers, and is usually disruptive and inconvenient to cardholders. Prior to a mass reissuance of identified at-risk card numbers, Visa suggests that issuers first evaluate the following:

- Fraudulent transactions that have been confirmed on the account
- Prioritized high-risk decline transactions – If the cardholder does not recognize the attempt, then replace the card
- Account pools that have confirmed fraud exceeding issuer thresholds
- Accounts with the highest fraud risk using a fraud score engine (e.g., VAA score) in combination with exposure (e.g., credit limit and/or open balance)
- Accounts with an expiration date in the near future – Since expired cards have no value to criminals, fraud activity on cards that are due to expire can be higher
- Accounts with a high Compromised Account Risk Condition Code (CARCC), a Visa-generated risk assessment of the probability of a compromised account turning fraudulent in the next 30 days

The decision to reissue any card is based on a number of considerations, but ultimately belongs to issuers. A single data breach event may impact issuers differently, and thus, issuers must consider fraud protection protocols that will be most effective for them and their clients. Some factors to consider when setting fraud protection protocols would be:

- Vulnerability of the population
- Level of disruption associated with a new card
- Number of customers that proactively call to request a new card
- Type of account (credit, debit, business, High Net Worth)

In the event it is appropriate to reissue a card, consider the Visa Account Updater (VAU) to help avoid disruption of recurring payments. Issuers should contact their Visa representative for more information.

Report Fraud

All fraud should be reported to Visa completely and accurately within 90 days of occurrence. Additionally, for fraud to be considered under the Global Compromised Account Recovery Program, issuers must report fraud on an account within 120 days of the PA, IC, or RA CAMS alert in which the account was first communicated to the issuer.