The Future of Payment Security in Canada

VISA

October 2017

Notices

Forward-Looking Statements

This presentation contains forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms "objective," "goal," "strategy," "opportunities," "continue," "can," "will" and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our corporate strategy and product goals, plans and objectives. By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. These forward-looking statements are based on our current assumptions, expectations and projections about future events which reflect the best judgment of management and involve a number of risks and uncertainties that could cause actual results to differ materially from those suggested by our comments today. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors. You should review and consider the information contained in our filings with the SEC regarding these risks and uncertainties. You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement, because of new information or future developments or otherwise.

Third Party Mark Notice

All third party brand names and logos used in this presentation are the property of their owners and are used for identification purposes only without endorsement.

Copyright Notice

Current Fraud Landscape

Current Fraud Landscape

For over 60 years, Visa has worked collectively with the industry to bring down fraud and keep it down. Technology has played a large part in that decline, from online authorizations to the global adoption of chip technology. While fraud remains low – roughly seven cents for every $100 transacted[1] – we are starting to see the impact of data compromises on fraud rates. The global fraud mix continues to shift to the card-not-present (CNP) channel (fraud conducted via online or over the phone transactions).

Between 2006 and 2016, CNP fraud through VisaNet increased from 35% to 57%[2].

What is 3D Secure?

3DS is a global industry protocol that provides mechanism for cardholder authentication at the time of an eCommerce purchase.

This is echoed in the Canadian fraud landscape:

Card-not-present fraud accounted for 78% of all fraud perpetrated on Canadian accounts month ending March 2017[4].

60% of card-not-present fraud losses on Canadian accounts are perpetrated outside of Canada month ending March 2017[1].

74% of fraud losses at Canadian merchants are perpetrated in the CNP channel, in the month ending March 2017[1].

Over 97% of card-not-present fraud occurs on transactions where enhanced authentication through 3D Secure (3 Domain Secure) is not enabled[3].

Counterfeit fraud on Canadian Visa accounts, accounting for 11% of fraud dollar losses month ending March 2017 and decreasing year-over-year, due to the successful implementation of EMV chip technology on cards and terminals in Canada[1].

Cross-border counterfeit fraud, where Canadian issued cards are used outside of Canada, is also on the decline due to the rapid adoption of EMV terminals in the United States[1].

[1] Source: Visa Fraud (TC40) Reporting and Sales September 2017
[2] Source: VisaNet settlement data December 2016
[3] Source: Visa e-Commerce Volume and VBR penetration dashboard – June 6 2017
[4] Source: Fraud Performance Benchmarking (FPB). TC40 fraud reported by Issuers and VisaNet Settlement data - 2017

Current Fraud Landscape

Over the past eighteen months, Visa led a cross-functional working group including clients and industry stakeholders to help inform the key elements of our roadmap and align to our shared goals of addressing card-not-present growth and securing data. The following elements, phased in over time, resulted from that consultation.

Strategic Pillars	Data Security		Fraud Prevention	
	Devalue	Protect	Harness	Empower
	• No fallback to magnetic stripe • 100% EMV Chip enabled point-of-sale • Tokenization	• PCI DSS version 3.2	• Dynamic Risk-based Authentication (3DS 2.0) • Expanded use of CVV2 • Authorization enhancements	• Consumer Alerts • Global Registry of Service Providers

1. Devalue Data

1. Devalue Data

No fallback to magnetic stripe at an EMV Chip Enabled Point-of-Sale (POS)

Where are we now?

A 'fallback' transaction occurs when a chip card being used at a chip-enabled terminal cannot be read due to a technical issue with the chip, or issues with the terminal. When the chip cannot be read, the technology "falls back" to a magnetic stripe transaction. This situation occurs infrequently since EMV chips on cards rarely fail. The fraud rate for magnetic stripe fallback transactions is significantly higher than a chip transaction[1].

[1]Source: Visa Fraud (TC40) and Settlement Data Q4' 2016

Where are we going?

To further protect transactions in the card present space, Visa is implementing a change that will require Visa issuers to decline chip card transactions at a chip-enabled terminal that are processed as a magnetic stripe transaction.

Requirements

Effective 14 April 2018, if an EMV chip card is not functioning properly at a chip enabled merchant and the merchant attempts to process the transaction by swiping the magnetic stripe, the issuer must decline the transaction.

1. Devalue Data

100% EMV Chip-Enabled Point-of-Sale (POS)

Where are we now?

The introduction of chip technology (EMV) enhanced security paved the way for innovations like contactless and mobile payments. Chip cards generate a unique one-time code each time they're used in-store at a chip-activated terminal. Unlike mag-stripe cards, this feature is virtually impossible to duplicate in counterfeit cards, preventing in-store fraud from occurring.

To further secure the ecosystem, In March 2011, Visa introduced the liability shift policy. This policy encourages merchants to accept chip card transactions by making merchants liable for any resulting counterfeit fraud in the event they don't accept this form of payment.

Almost 93%[1] of Canadian-acquired card present transactions are a chip transaction as of July 2017. A small number of merchants have yet to adopt chip technology terminals and are putting consumers at risk.

[1]Source: Authentication Implementation Monitoring Dashboard (May-July 2017)

Visa's Zero Liability Policy

All Visa transactions today — chip and non-chip — are safeguarded through Visa's Zero Liability Policy, which protects Visa accountholders from being liable in the event of fraud.

Where are we going?

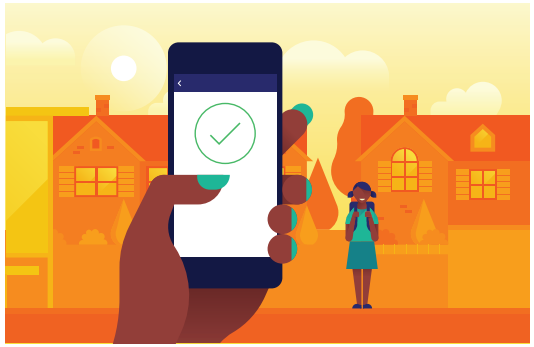
We believe that protecting merchants from loss is good for business. Therefore, we intend to advocate for the elimination of mag-stripe transactions, moving to 100% EMV-enabled terminals, ATMs and accounts issued in Canada.

Requirements

Effective 14 October 2020, all merchants must be EMV chip-enabled, with the exception of unattended cardholder-activated terminals (UCAT) merchants. UCAT merchants will have to be EMV-enabled by 14 October 2022.

1. Devalue Data

Tokenization



Credential-on-file

Growth in digital commerce and the emergence of new business models have led to an increase in consumer transactions where cardholders' payment credentials (e.g. account number or token) are on file with the merchant, digital wallet provider or other service provider, so that those credentails can be used seamlessly for future transactions.

Where are we now?

In 2013, Visa led a global industry collaboration on tokenization and was integral to the development of the EMVCo tokenization specifications. Tokenization is an industry wide initiative that brings an added layer of security to mobile and digital payments, preventing cross channel fraud without adding friction to the shopping experience.

It was designed to be interoperable and limit ecosystem changes. The security objective of any tokenization process is to replace account holder information such as account numbers and expiration dates with a unique digital identifier (a "token"). Such a token can be unique to a device, wallet provider or use case, such as credential-on-file.

Where are we going?

The Visa Token Service (VTS) uses the EMVCo specifications to provide a service for Visa's issuers, acquirers, merchants and processors to be able to implement network tokenization services for Visa accounts. Presently, VTS supports issuer wallets and third-party wallets such as Apple Pay™, Samsung Pay™ and Android Pay™.

Tokens will be a key enabler of embedded payments in Internet of Thing (IOT) devices and wearables, such as Garmin Pay™.

2. Protect Sensitive Data

2. Protect Sensitive Data

PCI DSS Version 3.2

Where are we now?

PCI DSS compliance is the foundation of Visa's Data Security and Compliance programs and is critical to protecting sensitive account-holder data from compromise. PCI DSS set the technical and operational requirements to help organizations — merchants, financial institutions, payment processors, service providers and technology providers — keep their cyber defences primed against attacks aimed at stealing account-holder data.

Where are we going?

The PCI Security Standards Council (PCI SSC) published new data security standards in April 2016 – PCI DSS version 3.2 (from version 3.1) to address growing threats to customer payment information. Companies that accept, process or receive payments should adopt version 3.2 to prevent, detect and respond to cyber-attacks that can lead to breaches.

2. Protect Sensitive Data

Contactless Magnetic Stripe Data (MSD)

Where are we now?

Early implementation of contactless acceptance was based on Magnetic Stripe Data (MSD) contactless terminals. Most contactless terminals in Canada now support both MSD and quick Visa Smart Debit / Credit (qVSDC) transactions.

An MSD contactless transaction means the terminal reads the EMV contactless chip, but processes the transaction as a magnetic stripe transaction.

Currently, the Visa rules require that EMV contactless terminals deployed in Canada comply with Visa Contactless Payment Specification and be capable of processing transactions using both paths.

Where are we going?

Visa has been alerted to fraudulent activity in which criminals emulate contactless transactions.
The fraudsters use a mobile application to emulate Visa MSD contactless magnetic stripe transactions and use the device at merchants with contactless acceptance.

To avoid this risk, contactless acceptance devices in Canada will no longer support the MSD transaction path.

Requirements

Effective 19 October 2019 all contactless acceptance devices in Canada must not support the MSD transaction path.

3. Harness Data

3. Harness Data

Dynamic Risk-based Authentication (3DS 2.0)

Where are we now?

Three-Domain Secure (3DS) is a messaging protocol that enables consumers to directly authenticate their account with the account issuer when shopping online.

To date, 3DS in Canada has had a very low rate of merchant adoption (approx. 3.8%[1] as of July 2017) due to issues around friction for the consumer and the impact of this friction on shopping cart abandonment for merchants.

Canadian issuers have started to migrate from 3DS required specific password for every transaction to a risk-based authentication (RBA) model. As of April 2017, 62.2 %[2] of Canadian issuer accounts are RBA enabled.

[1] Source: Visa e-commerce volume and VBV penetration dashboard – 6 June 2017
[2] Source: Visa Settlement Data August 2017

Where are we going?

Based on industry feedback, a new version of the 3DS (Version 2.0) was launched in October 2016 by EMVCo. The new version allows for a better user experience, supports mobile in-app and connected devices and richer data to enable robust, risk-based authentication decisions. The majority of transaction will not require any authentication by the cardholder. Issuers may require additional authentication for certain transactions. In those situations, 3DS 2.0 enables account-holders to more easily authenticate their identity in real-time with a dynamic password provided via mobile phone SMS or by a one-time password-generating token device.

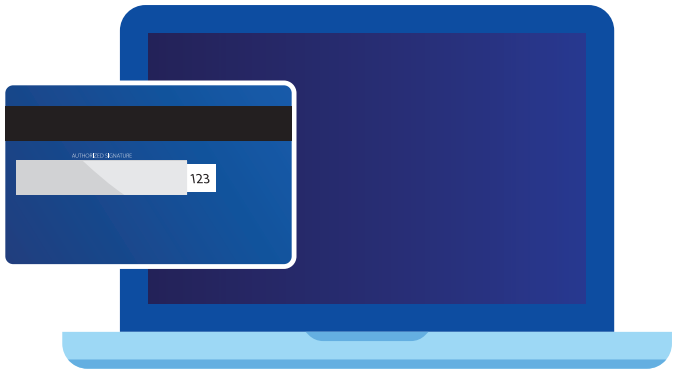
Requirements

Effective 14 April 2018, Visa will eliminate the use of 3DS specific static passwords and related enrollment processes.

Merchants that authenticate transactions using 3-D Secure are generally protected from issuer card-not-present fraud-related chargeback claims, and this rule will extend to merchant-attempted 3-D Secure 2.0 transactions after 12 April 2019, the global program activation date.

3. Harness Data

Expand the Use of CVV2



Where are we now?

CVV2 (Card Verification Value 2) is a three-digit number on the back of your credit or debit card that is used for authentication during a card-not-present (CNP) transaction.

Providing your CVV2 number to an online merchant proves that you actually have the physical credit or debit card - and helps to keep you safe while reducing fraud.

Where are we going?

To help address card-not-present fraud, Visa is implementing changes that expand the use of CVV2 for telephone or ecommerce merchants in Canada.

Using CVV2 provides card-not-present merchants protection from the account number and expiry date data that may be compromised in the card present channel since the CVV2 would not also be exposed.

Requirements

Effective October 14, 2017
All new ecommerce or telephone order merchants MUST capture the CVV2 and include it in the authorization request during a Visa transaction. (Not applicable for credential on file, recurring or installment payments, a Visa commercial card virtual account and digital wallet transactions)

- If an issuer approves a 'no-match' transaction (i.e a CVV2 is provided but it doesn't match the cardholder's account), then the issuer is liable for that amount. This offers an added layer of protection for merchants.
- All merchants in Canada will be prohibited from requesting CVV2 for mail order transactions if the data is provided in a written format. This reduces potential for that information to be stolen and used fraudulently.

These changes will be expanded to ALL ecommerce and telephone order merchants in Canada by October 13, 2018.

3. Harness Data

Authorization Enhancements

Where are we now?

As the payment system has evolved, instances in which a transaction is initiated with a stored credential based on a cardholder's consent for future use, have increased to significant levels.

Growth in digital commerce, together with the emergence of new business models, has increased the number of transactions a cardholders' payment credentials is stored for future purchases.

Recognizing stored credential transactions allow for better transaction risk evaluation, enabling robust processing and resulting in differential treatment.

Requirements

Effective October 2017:
Merchants and their third-party agents, payment facilitators, or stored digital wallet operators that offer cardholders the opportunity to store their credentials on file must:

- Disclose to cardholders how those credentials will be used.
- Obtain cardholders' consent to store the credentials.
- Notify cardholders when any changes are made to the terms of use.
- Inform the issuer via a transaction that payment credentials are now stored on file.
- Identify transactions with appropriate indicators when using stored credentials.

What is a Stored Credential?

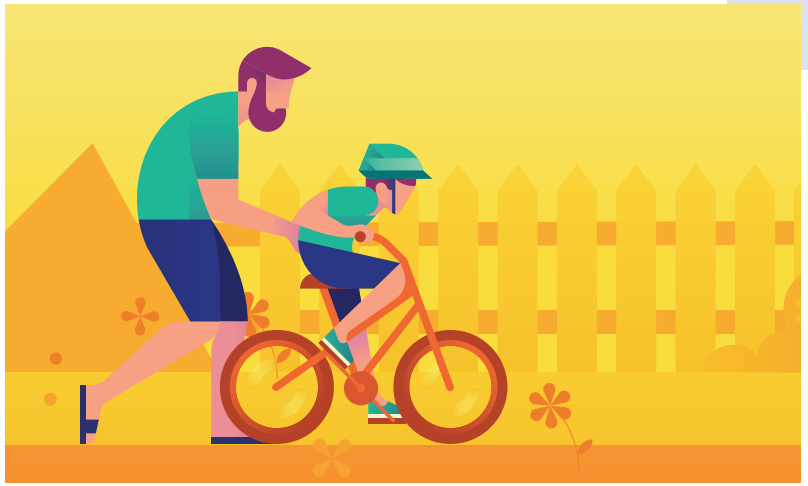
A stored credential is information (including, but not limited to, an account number or payment token) that is stored by a merchant or its agent, a payment facilitator, or a staged digital wallet operator to process future transactions.

4. Empower Everyone

4. Empower Everyone

While Visa and the payments industry has a number of initiatives in place, the first line of defense against payments fraud is for merchants and consumers to be well informed so they can take action to prevent fraud.

Visa has developed fraud prevention tools for consumers, banks and merchants to be better equipped in combatting fraud.



For Consumers:

All Canadian issuers can provide consumer Visa credit, debit and reloadable prepaid cardholders with an option to enroll in transaction alerts. This means that every time a consumer card is used, they could receive a message from their issuer, allowing for almost immediate notification of any fraudulent transactions.

Requirements

Effective 13 October 2018, all Canadian issuers to provide consumer Visa credit, debit and reloadable prepaid cardholders with an option to enroll in transaction alerts. This requirement is applicable to all Visa-branded card authorizations that are processed by Visa, Interlink and Plus; it is not applicable to non-reloadable prepaid cards or to any commercial cards.

Global Registry of Service Providers for Banks & Merchants

Protecting the data that is stored in or flows from your point-of-sale system to your acquirer is key to earning and keeping the trust of your customers. The Visa Global Registry of Service Providers is available to help ensure you have qualified agents working to secure your data. Banks and merchants should reference the site www.visa.com/splisting regularly as part of their due diligence process, and should only use service providers that are listed on the Registry for outsourcing their payment-related services.

Conclusion

Conclusion

Canada Payment Security Roadmap

2017

Expand use of CVV2

- New telephone and e-commerce merchant must submit CVV2 in the authorization
- Non-match approval liability shift
- Mail order merchants must not use CVV2 in paper format

2018

Expand use of CVV2

- All telephone and e-commerce merchant must submit CVV2 in the authorization

Expand use of 3DS

- Issuers eliminate the use of static passwords for 3DS
- Awareness and education on 3DS v2.0

Consumer Alerts

- Issuer must provide a consumer alert service

Chip Fallback

- Issuers must decline fallback to magnetic stripe for domestic transactions

2019

Expand use of 3DS

- Global 3DS 2.0 program activation

Contactless MSD

- Canadian merchants must not accept Magnetic Stripe Data (MSD) contactless transactions

2020+

EMV Chip

- All Canadian merchants must be EMV-enabled by 2020 and UCAT merchants by 2022

Conclusion

Visa collaborates with industry stakeholders, policymakers, law enforcement and consumers to keep payments secure and prevent fraud. We deploy a multi-layered security approach that has kept fraud rates low, despite significant growth in electronic payment volumes.

Our Canadian Security Roadmap focuses on four pillars:

1. Devaluing data by removing sensitive data from the ecosystem and making stolen account details useless (no Fallback, 100% EMV chip-enabled terminals and tokenization).
2. Protecting data by implementing safeguards to protect personal data as well as account details (PCI DSS 3.2, removing Magnetic Stripe Data support).
3. Harnessing data by identifying potential fraud before it occurs and increasing confidence in approving good transactions (3DS 2.0, CVV2)
4. Empowering everyone including consumers and merchants to fight fraud.

Visa is one of the most secure and trusted ways to pay and be paid. With any new technology, security will continue to evolve based on the needs of consumers and the dynamics of the marketplace. While some of the concepts outlined here are real and in market, others are an articulation of the possible, based on what is available today. As technology continues to shape our industry, Visa will continually update this security roadmap to address new and evolving risks. This is a dynamic industry and Visa is committed to staying at the forefront and adapting to the needs of consumers, issuers, acquirers and merchants, as we bring digital payments into the everyday, making digital payments more secure for everyone, everywhere.