NORTH AMERICA INSIGHTS

MARCH 2023

Securing the digital economy

Why employing proactive cybersecurity can save consumers and businesses millions of dollars

Our world is more interconnected than ever before. Digital advancements from AI to the metaverse are creating new opportunities for digital payments and e-commerce. In 2021, global ecommerce growth rates exploded to reach 17.1%, one of the largest spikes in recent history, fueled by the pandemic.[1] However, these advancements in technology and associated user behaviors are accompanied by undeniable security risk.

Consumers are facing threats at every turn with bad actors and cybercriminals constantly developing new techniques for stealing personal and financial data. Social media, the dark web e-commerce and other platforms further proliferate the accessibility of stolen information. Proper cyber hygiene is also not regularly employed by consumers, with about only half changing passwords when prompted by a platform, when hacked, or not at all; the same percentage often reuse the same password on most of their accounts.

Cybersecurity is an issue impacting individuals and organizations around the world. According to the World Economic Forum's Global Cybersecurity Outlook 2023, 93% of cybersecurity experts and 86% of business leaders believe global geopolitical instability is likely to lead to a catastrophic cyberattack in the next two years. Additionally, they acknowledge the lack of skilled cyber experts as a threat to business and society, with key sectors such as energy and utilities reporting a 25% gap in critical skills.[2] According to recent estimates, the current worldwide cost of cybercrime is $6 trillion, accounting for 1% of the global GDP; this estimated cost will rise by $4.5 trillion in the next few years.[3]

For most businesses, it's not a question of if a data breach or fraud will occur, but when. Younger businesses under five years old are more likely to report being hacked, resulting in the loss of highly sensitive financial, employee and payment card information. The consequences can be incredibly costly, especially for North American business leaders, with the average cost of data breaches in the U.S. and Canada estimated at $9.4 million and $5.64 million respectively (global average is valued at $4.34 million).[4] Despite those costs, business leaders do not invest in proactive defense for their businesses - only 39% have implemented ongoing vulnerability assessment tools.

In the face of these threats, Mastercard aims to evolve alongside our interconnected world, with providing safety, security and peace of mind for our customers and partners. Join us in learning more about the security landscape and mindset of today's consumers and business leaders, as well as the ways in which we can leverage proactive risk assessment and reliable data security tools. We hope these insights equip you for upcoming shifts and motivate you to act upon the security imperative.

Together, we can build a secure digital future that everyone can trust.

Les Matthews
Executive vice president, head of services for North America

For more information, contact:

Diego Szteinhendler
Senior vice president
North America
Cyber & Intelligence solutions
diego.szteinhendler@mastercard.com

Ranjita Iyer
Senior vice President
Business development
Cyber & Intelligence solutions
ranjita.iyer@mastercard.com

Dana Farber
Director
North America insights
dana.farber@mastercard.com

Contents

1 Our interconnected world creates new vulnerabilities and costs

Recent years have seen an enormous spike in cybercrime, which is estimated to have increased by 600% since the pandemic.[3] Remote work has particularly created vulnerabilities, resulting in a 238% rise in cyberattacks.[5] This rise in crime equates to a rise in cost. According to recent estimates, the current worldwide cost of cybercrime is $6 trillion, accounting for 1% of the global GDP; this estimated cost will rise by $4.5 trillion in the next few years.[3]
As a result of this increased risk, consumers and business leaders are most concerned about security threats that expose identifiable information, like identity theft, hacking and fraud.

2 Consumers are trying to balance security and convenience

Over half of consumers have already experienced some form of digital security issue; this vulnerability isn't always the fault of bad actors. Despite satisfaction with current password management and reported use of two-factor authentication, about half of consumers (45%) only change passwords for providers when prompted by the platform, when hacked, or not at all, with a similar percentage (44%) often reusing the same password on most of their accounts, leaving account information unprotected. This could be aided by password management technology, as 64% of consumers feel comfortable logging in with a regularly changing authentication code.

3 Business leaders need ongoing security solutions

Businesses are a major target for attacks, putting them at risk of financial loss, reputational damage and more. Younger businesses (those that are less than five years old) report greater vulnerability of being hacked. While most business leaders have implemented security solutions or conducted a digital risk assessment at a point in time, they neglect to implement ongoing solutions. Long-term security solutions like vulnerability assessments are leveraged by only 39% of business leaders, and even fewer use phishing solutions (34%), leaving major gaps in protection efforts.

4

New technologies elicit uncertainty, but also opportunity

Consumers anticipate they will be grappling with new privacy issues, as the types of information and the technology transmitting it become more sophisticated. Consumers' top concerns in the next five years include: misuse of biometric data, facial recognition software and genetic information. However, these types of data also provide new opportunities for securing their personal information and transactions. Nearly six in 10 (58%) are interested in using biometrics (fingerprint and face-based) as more secure alternatives to passwords, and the same number wish more platforms offered biometric security.

5

Financial service providers must act as leaders in the security space

Keeping data safe provides a security guarantee to consumers and businesses alike. Over half of consumers believe that financial services are responsible for preventing data breaches, with the same number wanting preventative measures through data encryption. Financial services providers can use resources they already have, like leveraging alerts to consumers at ease, as well as encourage them to develop better cyber hygiene habits. Financial institutions can also create security in new financial frontiers; most business leaders and consumers trust financial institutions, like banks and payment networks, to provide secure payments in the metaverse.

About the research

In the fall of 2022, The Harris Poll, in partnership with Mastercard, conducted two, large-scale, surveys. The first, taken from October 26 to October 31, involved 4,009 individuals, of which 2,007 were from the U.S. and 2,002 were from Canada.

The second survey, conducted from November 9 to November 14, involved 502 business leaders, of which 400 were from the U.S. and 102 were from Canada. (To qualify for the survey, respondents had to be a decision maker at their organization both generally and for security strategy, own a credit card or debit card that they use for business expenses and work for a business that makes a revenue of $10 million or more).

The findings from the aforementioned surveys were also complemented with expert interviews and industry-landscaping research. This research was conducted by The Harris Poll, led by Abbey Lunney, Morgan Rentko and Saskia Gregg. For more information about The Harris Poll, please reach out to abbey.lunney@harrispoll.com

Part 1: Exploring an evolving security landscape

Navigating an interconnected world

"Working from home brought [cybersecurity] to bear with us the exchange of knowledge, ideas, [and] threats increased awareness, investment and prevention measures that were put in place."

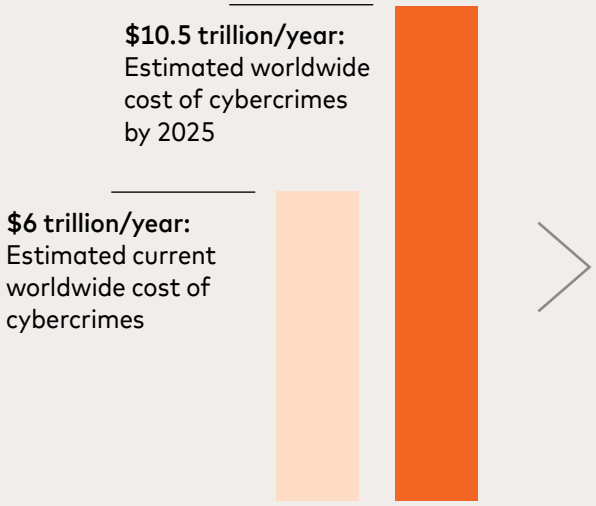
– Risk management consultant, (financial services, defense and information technology experience)

Digital security is more essential than ever in 2023, as our professional and social lives are online. Being part of an increasingly digital sphere is beneficial, enabling us to form relationships with people far and wide, dive head-first into exploring new worlds and participate in the digital economy. However, the interconnected nature of our world also generates glaring vulnerabilities and costs.

One particular vulnerability in our current world is hybrid and remote work. Since more employees are working hybrid schedules or completely from home, they may not be engaging in optimal security practices; unsecured home networks and the use of personal devices for work purposes make remote employees more vulnerable to cyberattacks. There has been a resulting 238% rise in cyberattacks compared to pre-pandemic.[5]

The frequency of cyberattacks are not the only numbers that are climbing. According to recent estimates, the current worldwide cost of cybercrime is $6 trillion, accounting for 1% of the global GDP.[4] These numbers are expected to rise dramatically, with the estimated cost increasing by $4.5 trillion in the next few years.[4]

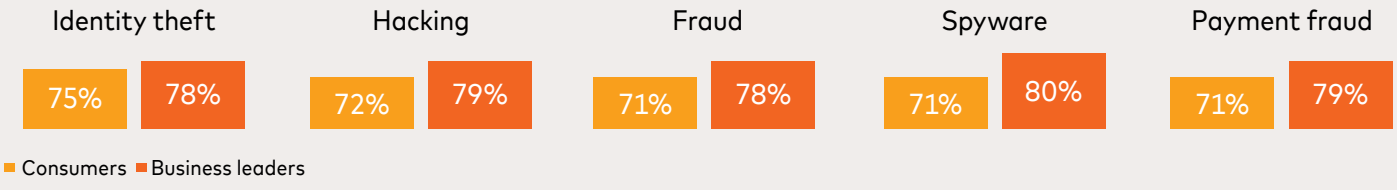
Consumers and business leaders are most concerned about security threats that expose identifiable, sensitive information, like identity theft, hacking and fraud.



Cybercrime has increased by 600% since the pandemic[4]

The value of cybercrime cost accounts for 1% of the global GDP[4]

Concern about digital security threats:



Recognizing rising consumer threats

"I don't feel adequately protected from cyber threats. [I] change my passwords and make them challenging; however, I have so many and forget them."

– Consumer interview, director of education in FL

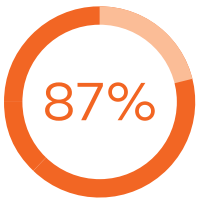
"[There's] always been this balance between convenience, security and privacy. People want it to be quick and easy, but also safe and secure. Ultimately, you are putting something that's worth something to you somewhere, whether it's in a bank vault or a digital sphere."

– Chief risk officer at a credit union

Consumers are reckoning with the inherent risk associated with conducting much of their lives online. Whether it's phone scams, phishing, or payment fraud, over half have already experienced a digital security issue in their lifetime. Digital security threats that expose personal information, including identity theft and hacking, are top of mind for consumers today.

When bolstering digital defense against bad actors, consumers must take personal cyber hygiene practices into account. For instance, most consumers are satisfied with their current password management habits and report implementing protective measures like two-factor authentication.

However, trying to balance security and convenience may contribute to unsafe shortcuts: about half of consumers (45%) only change passwords for providers when prompted by the platform, when hacked, or not at all. The same percentage (44%) often reuse the same password on most of their accounts, showing that consumers still require education on smart password creation or password management tools.



of consumers expressed concern about digital security threats
U.S.: 89% | CA: 86%

of consumers have experienced a security issue in their lifetimes
U.S.: 58% | CA: 53%

Password behaviors

77%
Use two-factor authentication on their online accounts

45%
Only change passwords for online accounts when prompted by the platform, when hacked, or not at all

23%
Change passwords for banks/credit card providers once a month / every few months

26%
Change passwords for banks/credit card providers a few times a year / once a year

24%
Change passwords for banks/credit card providers only when prompted by the platform

Protecting digital payments

8.1%

Increase in e-commerce from 2018 to 2022[6]

69%

of consumers are likely to use a digital wallet (e.g., PayPal, Amazon Pay, etc.) to avoid account numbers being shared directly with retailers

U.S.: 69% | CA: 68%

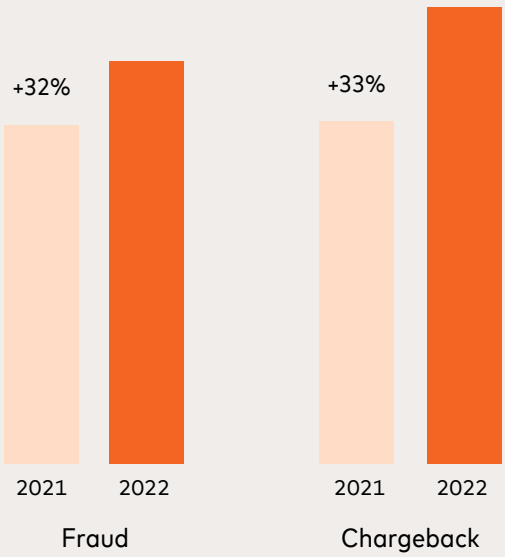
Whether making a mortgage payment, picking up a coffee or ordering groceries online, consumers are making digital payments part of their everyday life. In recent years, consumers have been increasingly leveraging e-commerce for their purchases. In 2018, online sales made up 10.2% of total retail sales – but in 2022, online sales accounted for 18.3% of total retail sales, an increase of 8.1% in just four years.[6]

When conducting online transactions, consumers are keeping security in mind. Nearly seven in 10 (69%) are likely to use PayPal or a similar service to avoid their account numbers being shared directly with retailers and the same percentage (70%) would rather use guest checkout so they don't have to provide email information. Many consumers are also bypassing the convenience of saving payment information, as about six in 10 (57%) are unlikely to save their credit card information on a retailer's website.

Consumers are also considering the impact of in-store payments, even when it comes to digital payment methods. Over half (55%) are currently worried about having their credit or debit card information stolen after using a digital wallet/contactless credit card to pay in store.

Consumers are right to be concerned; as digital transactions grow, so has fraud. Over the past year, Mastercard has observed fraud increase 33% and chargebacks increase 32% on their network in the U.S. market.[7]

YOY Fraud and chargeback growth in the U.S.



Identifying business vulnerabilities

$9.4 million

Average cost of a data breach in the U.S. ($5 million more than global average) [3]

$5.64 million

Average cost of a data breach in Canada ($1 million more than global average) [3]

Because cyberbreaches are largely motivated by financial gain, businesses are a major target for attacks, putting them at risk of financial loss, reputational damage and more. Businesses less than five years-old tend to report a higher rate of being hacked, resulting in loss of highly sensitive financial, employee and credit/debit card information.

Data breaches have consistently resulted in personal and professional fallout for almost all business leaders who have experienced them. Ramifications include the loss of customer data and the need for reactive security measures, as well as personal stress and the loss of customer and vendor relationships.

For North American business leaders, security risks can be especially costly. The average costs of data breaches in the U.S. and Canada are millions above the global average of $4.34 million. In addition, data breaches frequently come at the customer's expense, as 60% of organization's breaches led to increases in prices passed on to customers.

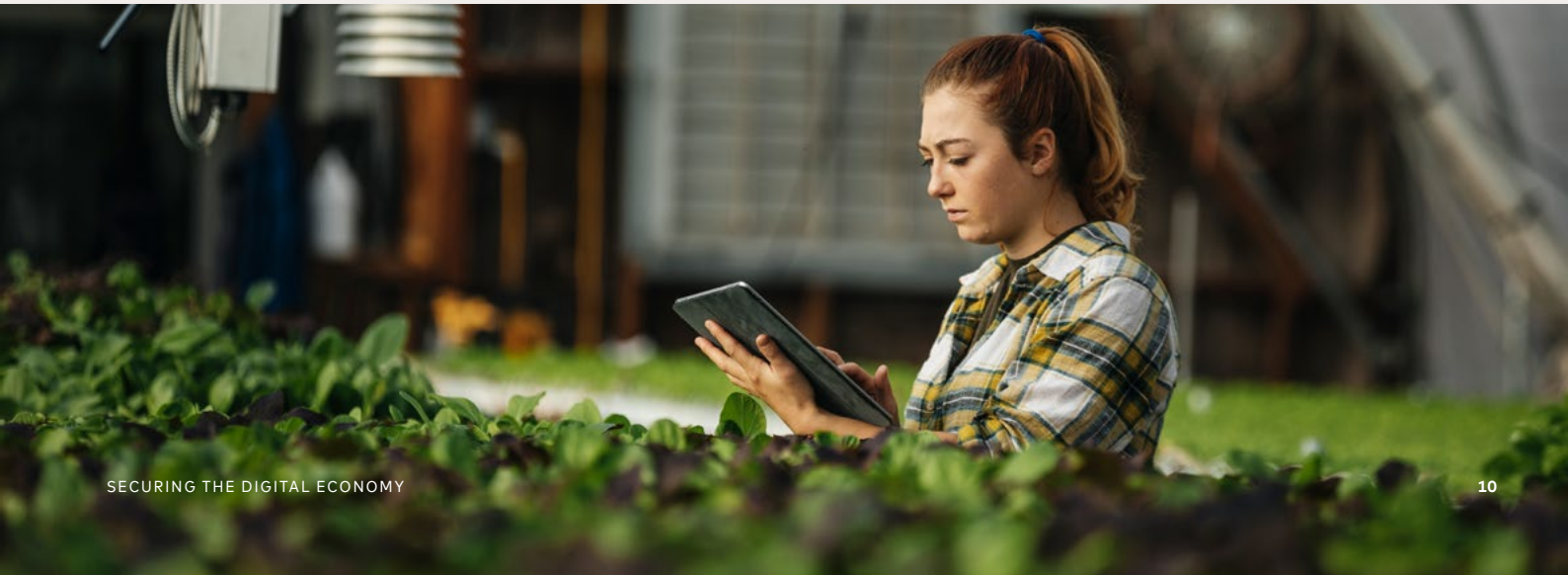
of business leaders who have been hacked say it has impacted them/ their business in some way

Top three business ramifications:

1. Lost customer data	30%
2. Hired security consultants	30%
3. Signed up for more employee security training	29%

Top three personal ramifications:

1. Was stressed at home/with others	44%
2. Lost or strained relationships with vendors	38%
3. Lost or strained relationships with customers	34%



PART 1: EXPLORING AN EVOLVING SECURITY LANDSCAPE

92%

of business leaders have implemented security solutions or conducted a digital risk assessment at certain points in time

39%

of business leaders have ongoing vulnerability assessment tools (e.g., RiskRecon) implemented at their business

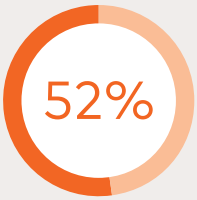
Business leaders need to protect their payment processing services (e.g., Square) and digital financial tools (e.g., online banking), which are most vulnerable to threats. While most business leaders have implemented security solutions or conducted a digital risk assessment, they neglect to take ongoing action, which leaves them vulnerable to cyberattacks.

When examining the top security solutions implemented at businesses, leaders are opting for initial lines of defense like antivirus software and firewalls, which are leveraged by over half of business leaders. Meanwhile, long-term security solutions like vulnerability assessments are leveraged by only 39% of business leaders and even fewer (34%) use phishing solutions. This leaves major gaps in protection efforts and shows the need for a proactive strategy in place of a reactive one.

Another gap lies in the staff tasked with security. Six in 10 business leaders have internal staff managing security protocol and training employees on security best practices, but this likely isn't their full-time responsibility within the company, but only 46% have hired a third-party IT and security team dedicated to proactive security work.

Top security solutions used at businesses

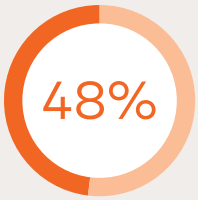
Network firewalls



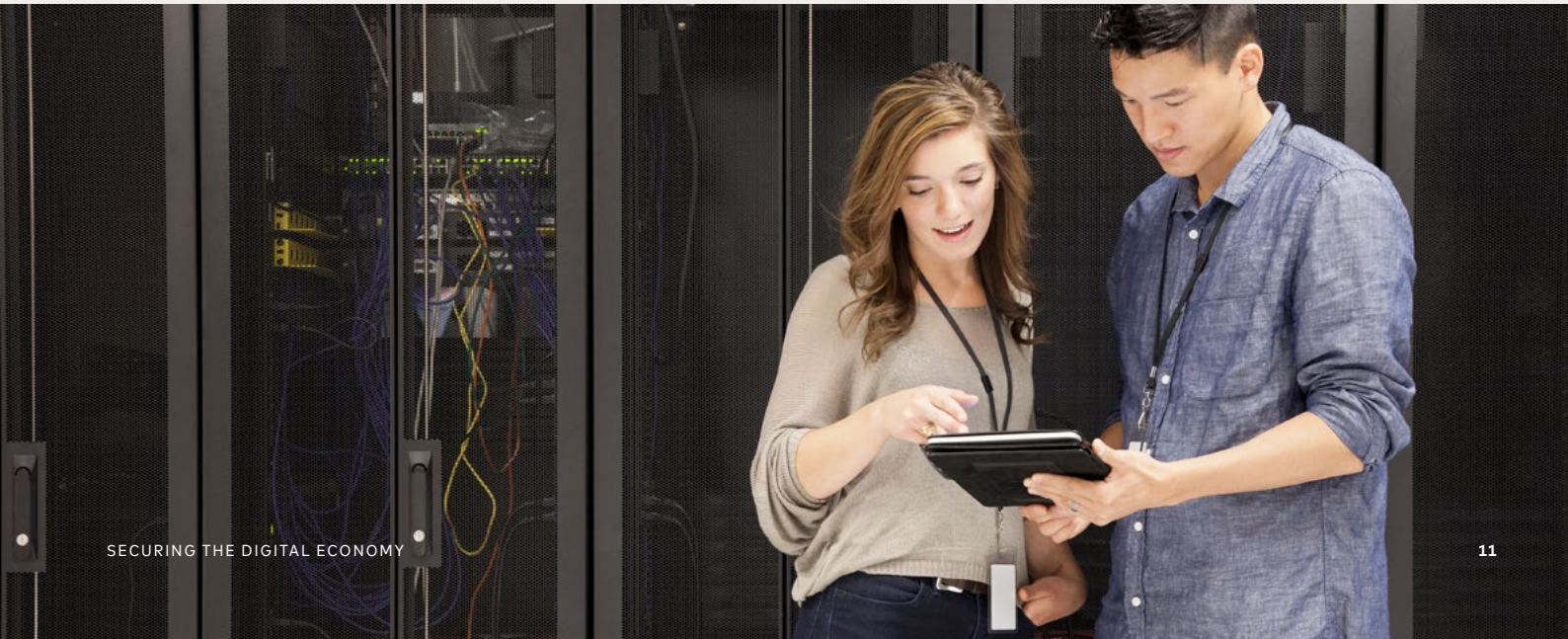
Two-factor authentication

Antivirus software

Fraud protection



Cybersecurity insurance



Part 2: Anticipating shifts in security

Assessing privacy concerns

34%

agree the individual has the most control over personal data

U.S.: 33% | CA: 34%

"Before the pandemic, I did not see vulnerability in storing or using my debit or credit cards on websites or using my physical cards in person. I've had my personal information and identity stolen many times since then which has caused me to become more aware"

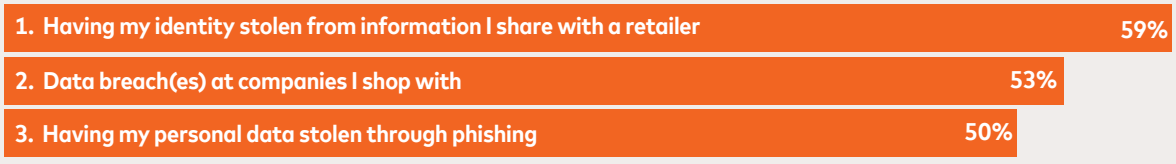
– Consumer interview, executive administrator in NY

The rise of high-profile data breaches and complex cyberattacks are driving consumers to evaluate their approaches to personal data protection. The vast majority want the ability to 'opt in' or 'opt out' of their data being used, shared, or sold by companies – and about three in 10 consumers do not feel comfortable sharing any information at all with companies today.

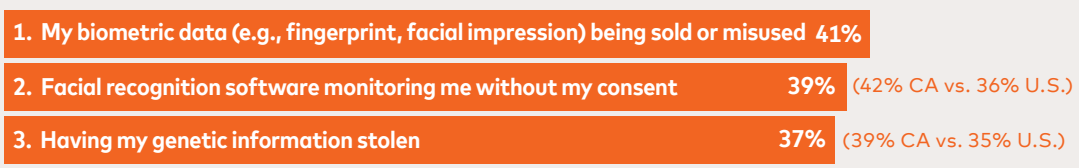
However, declining to share one's personally identifiable information may not be enough to guarantee security in the years ahead, and consumers may not be able to 'opt in' or 'opt out' of certain kinds of data. Consumers imagine they soon will be grappling with new privacy issues as types of information and technology transmitting it becomes more sophisticated.

Today's primary data worries include identity theft / data breaches at retailers and stolen personal information through phishing. When asked to look ahead five years, top concerns shift to misuse of biometric data, facial recognition software and genetic information, as consumers start to navigate using these technologies in their everyday lives.

Top worries today:



Top worries in the next five years:



Guaranteeing data protection

91%

of consumers believe companies should spend more to protect consumers' data

U.S.: 89% | CA: 92%

81%

of consumers say if they don't trust a company to protect their data, they won't buy from them (no matter how great their products are)

U.S.: 81% | CA: 82%

52%

of consumers believe companies should encrypt all consumer data to increase protection

U.S.: 50% | CA: 55%

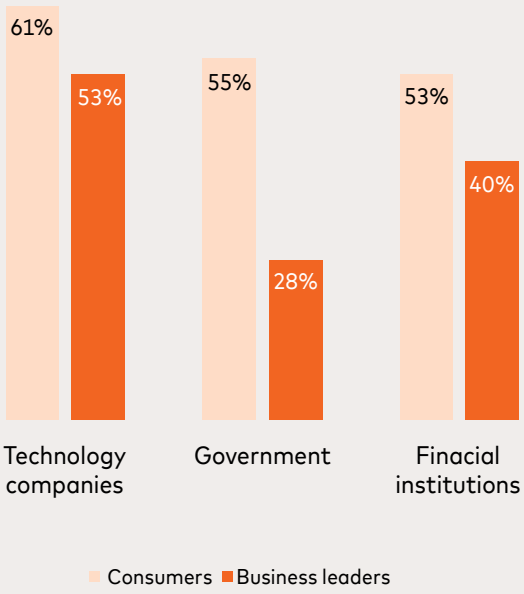
While personal cyber hygiene is undoubtedly necessary to consumer security, companies have a responsibility to keep consumer data safe. Promises to protect data aren't enough for consumers – they want a guarantee of data protection.

This guarantee starts with a proactive and preventative approach. Consumers and business leaders cite technology companies, the government and financial institutions (in particular, banks and payment networks) as top industries responsible for preventing data breaches. About two-thirds of consumers (63%) want these types of companies to proactively implement security features to ensure private data cannot be accessed by hackers. Half of consumers (52%) expressed interest in encryption as a means of better protecting consumer data.

If a breach does occur and data is not protected, those affected want a guarantee that they will receive recourse. If consumer information is sold without consent, 86% believe that companies should provide them compensation. This response does more than provide monetary value; about two-thirds of consumers (64%) would be more likely to trust a financial services provider that guarantees them compensation for any loss suffered because of a data breach.

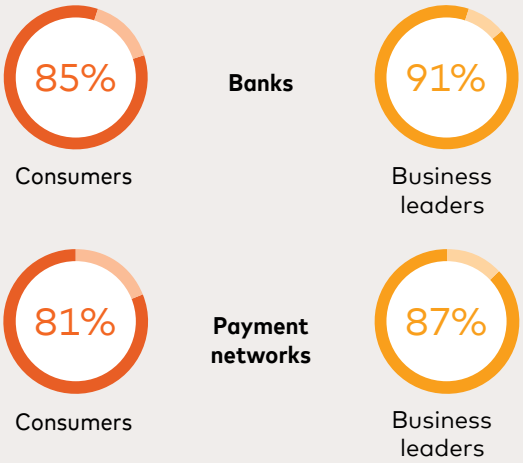
A guarantee of protection also requires trust, which is foundational to the way consumers will conduct their transactions. Most consumers (81%) say that if they don't trust a company to protect their data, they won't buy from them, no matter how great their products are. Younger generations are even more adamant on this principle: 46% of Gen Zs have already stopped interacting with a company because of a data breach.

Top industries responsible for preventing data breaches



Of those who found financial institutions responsible for data breaches

Financial institutions responsible for data breaches



Providing peace of mind through established and emerging tech

77%

of consumers feel comfortable with their bank monitoring account activity to provide possible fraud alerts

U.S.: 79% | CA: 75%

"I have been alerted that multiple websites that I was on as a teenager have been subject to data breaches and my old passwords may be compromised. My iPhone keychain notifies me if such an event may have occurred. I then go and either 1) delete a defunct account, or 2) change my password."

– Consumer interview, educator in CO

Promoting technology that is already leveraged by financial institutions can help put consumers at ease, as well as encourage better cyber hygiene habits. Seventy-seven percent of consumers feel comfortable with their bank monitoring account activity to alert them to possible fraudulent transactions, and the same percentage are already likely to receive phone alerts on credit purchases. Sound can also be an effective tool – 76% of consumers say that they feel more secure hearing a sound indicating a complete transaction, whether shopping online or in-store.

When it comes to logins and password protection, consumers are open to password management technology; sixty-four percent of consumers feel comfortable using an authentication code that regularly changes to log in (e.g., RSA SecurID). In addition, about one in four consumers only change their password when prompted by the platform; periodic password update prompts could also help consumers develop better habits.

Emerging technology should also be used to protect data. Consumers express particular interest in using biometrics (fingerprint and face-based) as more secure alternatives to passwords. Just over seven in 10 (71%) consumers already feel comfortable using their fingerprint to unlock their phone and 56% feel the same about FaceID. Over half of consumers (58%) wish more platforms offered biometric security, instead of passwords.

58%

of consumers would rather use biometrics than a password to protect their information

U.S.: 61% | CA: 56%

Comfort using the following technologies

76%

Bank monitoring account activity to alert of possible fraud transactions

71%

Using a finger to unlock phone

67%

Smart home security systems reporting suspicious activity

64%

Using an authentication code that regularly changes to log in (e.g., RSA SecurID)

56%

Using facial recognition to unlock phone

Shaping the safety of the metaverse

48%

of consumers have already participated in metaverse commerce (bought crypto or NFTs, attended virtual concert, bought virtual real estate, etc.)

U.S.: 52% | CA: 48%

"The only way to get cryptocurrency to scale is if banks adopt and make cryptocurrencies available. While a majority don't trust crypto, they do trust banks."

– Johan Gerber, EVP of Security and Cyber Innovation at Mastercard

The metaverse is fundamentally shifting how we interact with the world, bringing with it massive economic opportunity. According to recent estimates, the total addressable market for the metaverse economy could be between $8 trillion and $13 trillion by 2030, with up to five billion users.[8]

Nearly half (48%) of consumers have already participated in metaverse commerce, whether it's buying virtual real estate or investing in cryptocurrency. Despite this rising engagement, consumers are especially concerned with what the metaverse might mean for their finances and personal information.

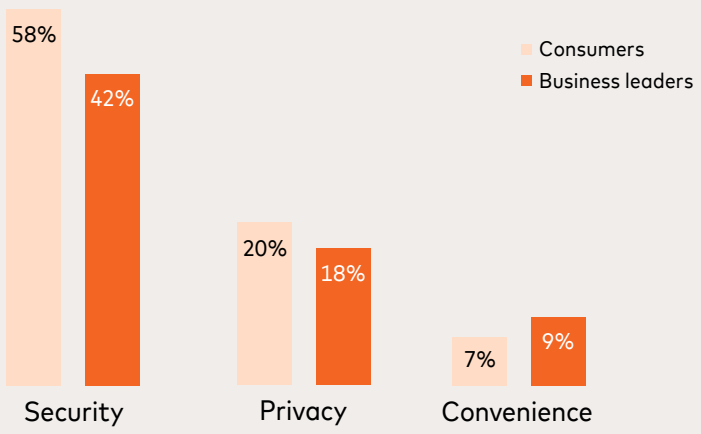
Security is the top need for digital payments in the metaverse for both consumers (58%) and business leaders (42%). When it comes to transactions, consumers are still most comfortable using traditional payment methods like credit cards (61%) and debit cards (54%) rather than in-game currencies (38%) and cryptocurrencies (31%) specifically built for virtual use.

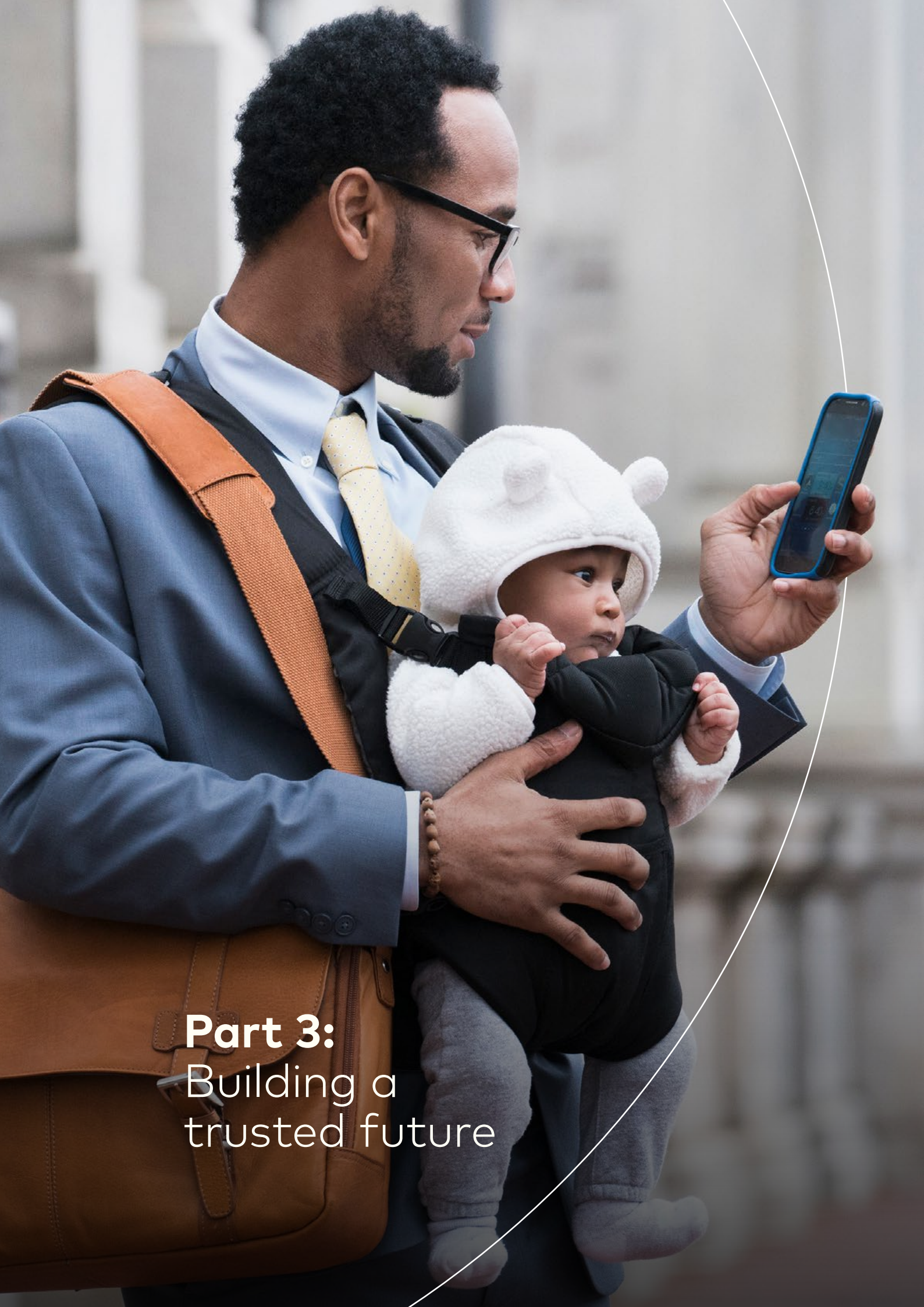
Business leaders and consumers see a path to digital payment security through financial institutions they know and trust. Business leaders are especially bullish about financial institutions' ability to strengthen digital payments, as the vast majority trust banks (90%) and payment networks (87%) to provide secure payments in the metaverse. Additionally, 9 in 10 (90%) business leaders would feel secure using cryptocurrency if their bank had an offering where they could invest in crypto, hold and manage actions through their bank.

While not at the same level as business leaders, most consumers (60%) still would be more interested in using cryptocurrency if it was backed by a trusted financial institution. They fundamentally believe that established leaders in financial services are the future of the metaverse; seven in 10 (68%) consumers think established financial brands should lead the way when it comes to payments in the metaverse.

of consumers would be interested in using crypto if it were backed by a trusted financial institution

Top three priorities for digital payments in the metaverse





Part 3: Building a trusted future

Five opportunities for brands to act on the security imperative

1. **Build cyber resilience** by conducting proactive vulnerability and risk assessments

2. **Leverage established technology** with timely alerts around transactions and information sharing

3. **Invest in biometric solutions** that will protect and optimize accounts and transactions

4. **Tap into trust** by guaranteeing accountability for potential data breaches and showing means of prevention (e.g., encryption)

5. **Open doors to the metaverse** by creating safe, trusted pathways for consumers to engage in metaverse commerce and crypto transactions

Opportunities to collaborate

Cybersecurity and risk management

Mastercard is committed to creating unique and essential solutions that support the institutions that service today's businesses. Our robust suite of cybersecurity products is designed to help business owners protect themselves and their customers against vulnerabilities.

Identity and account protection

A staggering percentage of financial institutions experience fraud when accounts are opened, while more than half cite identity theft as a major ongoing concern. Our solutions providing digital identity and device insights are designed to protect consumers at every stage of the account lifecycle, while facilitating digital onboarding without friction.

Transaction optimization

Mastercard leverages the latest technology driven by AL and ML to determine if a transaction is fraudulent — focusing on signals that allow merchants and issuers to increase approval rates while minimizing fraud and protecting cardholders. Post transaction capabilities increase transparency and enhance consumer experience.

Access and connectivity

Our intelligent network of services opens up new opportunities and efficiencies beyond the traditional transaction. By simplifying access to payments innovation to all payment networks, it allows you to differentiate your value proposition and increase profitability while focusing on your business.

Crypto and crypto risk

With Mastercard's worldwide network, we are helping make crypto accessible and secure for billions of consumers, businesses and governments.

1. Global E-commerce growth rate
2. Davos 2023: What you need to know about technology
3. Purplesec: Cybersecurity Statistics 2022
4. IBM: Cost of a data breach 2022
5. HP Wolf Security. 2022 Blurred Lines & Blindspots Report
6. Mastercard SpendingPulse Dec 2022
7. Mastercard Security Resiliency Program Overview 2023
8. Citi: Metaverse and Money Report 2022