WINNING NEW GENERATIONS WITH PERSONALIZED IDENTITY SECURITY
Traditional financial institutions (FIs) know that to remain relevant in the marketplace and compete with emerging financial technology companies and neo-banks, it’s important that they make their offering more appealing to a new generation of consumers. The challenge for some FIs is how to enhance their offering in a way that will add value and appeal to millennials and Gen Z consumers.

To help understand the relationship these consumers have with their financial institutions and what influences their financial decisions, BreachClarity — now part of Sontiq, a TransUnion company — conducted an online survey of 1,000 U.S. adults in May of 2020.* After analyzing the responses to that survey and incorporating insights from external research and news reports published throughout 2020, this paper was originally released in January 2021 and then updated in January 2022.

Within this competitive landscape, appealing to new generations of account holders requires a fresh but efficient approach. It should leverage the value of existing investments and be distinctly geared toward supporting younger consumers’ ability to meet their financial health goals safely and securely.

As a result of this analysis, several key findings stand out:

### KEY FINDINGS IN THE REPORT

- Millennials and Gen Z account for more than half the U.S. population with spending power of $3 trillion.
- Younger consumers value personalized service and are earlier adopters of advanced digital solutions.
- Advances in artificial intelligence (AI) now enable mid-market FIs to meet the high expectations of these consumers, creating a huge opportunity.
- As FIs seek to stand out when targeting these consumers, delivering hyper-personalized digital safety and security as part of financial health becomes critical.

* A nationally representative online survey conducted using Dynata, a global online market research firm. The margin of error for questions answered by the full survey population is +/- 3 percentage points at a 95% confidence level. The margin of error is higher for questions answered by smaller segments.
In less than a year, COVID-19 spread to every corner of the globe, hastening consumers’ digital adoption of financial services. Today, the traditional factors that some financial institutions once relied on to differentiate themselves from the competition have been replaced by modern preferences, making the ability to deliver all-new comprehensive and secure financial services through digital channels paramount to attracting new account holders.

Consumers have broadened and deepened their reliance on digital channels while eschewing storefronts, including those of financial institutions, where branch visits have declined by more than 50%.1,2 All the while, a vast new playground for cybercriminals has been built. Cybercrime has surged in recent years, severely affecting credit unions, banks and fintechs. These factors have driven financial institutions of all stripes to revisit their digital strategies and rethink what it will take to be successful going forward.

No groups have higher expectations for a digital experience than millennials and their younger Generation Z peers, who now make up more than 50% of the U.S. population3 and already have a combined spending power of nearly $3 trillion.4 While meeting their expectations isn’t always easy, doing so during this period of disruption presents a major opportunity for financial institutions to turbocharge growth.5

Financial institutions must deliver a personalized digital experience that empowers young consumers in every aspect of their financial health — with a special emphasis on identity safety. Although their parents and grandparents enjoyed decades of safe, trust-building relationships with their financial providers, young adults’ financial lives are being acutely shaded by cybercrime, just as they are building nest eggs, buying homes and managing the finances of their fledgling households for the first time.

1  S&P Global Market Intelligence, Annual Consumer Mobile Banking Survey, 2021
2  PYMNTS.com, Deep Dive: Why Self-Service Is the Rising Star of CU’s Branch-Based Banking Experiences, 2021
3  Brookings Institute, The Avenue: Now, more than half of Americans are millennials or younger, 2020
4  CreditUnionTimes, 3 Principles Credit Unions Should Adopt to Attract More Millennial Members, 2021
5  CU Collaborative, 9 Statistical Challenges for Credit Unions, 2018
IDENTITY IS PERSONAL

Individual identity is key for younger generations. No longer is there a driving need to fit in, but rather to stand out and be recognized. This is evidenced by the popularity of social media platforms that empower anyone and everyone to develop their own brand. Marketers for major brands are also heavily promoting the message that their products accentuate every young persons’ individuality. Not to mention that these generations are true digital natives, having been born into a world where the internet was pervasive. The combination of these two factors has fed the desire among younger consumers for the sort of personalized, digital services that many financial institutions have often struggled to provide.

Instead, in a world that is now barreling towards digital-first banking, it’s the large banks and so-called ‘challenger banks’ that are positioned to garner much of the attention from younger consumers. National institutions have invested heavily in digital channel capabilities over the years, while being able to attract new customers purely through the gravity created by their massive brands.

On the opposite end of the spectrum are digital-only banks that have packaged up a variety of financial health features in trendy packaging, all meant to appeal to different segments of young consumers. These well-funded challengers include venture capital-backed independents, subsidiaries of traditional institutions and non-bank fintechs.

Between technology and marketing, the remaining financial institutions are at a disadvantage. Reliant on legacy core providers that deliver one-size-fits-all digital banking experiences with ‘ecosystems’ of third-party apps which are often expensive to integrate, many are unable to deliver the type of personalized experiences that younger consumers expect. And marketing at these institutions typically emphasizes the sort of differentiators that younger consumers will not appreciate so early in their financial lives: great rates and personal service. This is why, for example, consumers under 35 are more than twice as likely to believe that their primary FI does not care about their financial health when compared to consumers between the ages of 35 and 54 (see Figure 1).

Within this competitive landscape, appealing to new generations of account holders requires a fresh but efficient approach. It should leverage the value of existing investments and be distinctly geared toward supporting younger consumers’ ability to meet their financial health goals safely and securely.

7. EMI, Investing in Digital Channels Generates Benefits for Banks...But They Should Not Abandon Human Channels, 2018
8. EY, NextWave Global Consumer Banking Survey, 2021
IDENTITY SAFETY:
A NEW KEY COMPONENT OF FINANCIAL HEALTH

The relationship between identity safety and financial health is straightforward. Financial health as defined by the Consumer Finance Protection Bureau (CFPB) has four criteria:

- Control over one’s finances,
- The capacity to absorb a financial shock,
- Being on track to meet financial goals and
- The ability to make choices that allows one to enjoy life.9

No matter the array of traditional financial health apps and services deployed by a financial institution, identity crime can potentially undermine a consumer’s ability to meet those financial health criteria.

The misuse of a consumer’s identity and accounts can take away any semblance of control while creating acute challenges to other areas of their financial health. For example, an account takeover can result in the temporary loss of savings that reduces a consumer’s ability to absorb financial shocks or make necessary purchases. In the case of fraudulent new accounts, the resulting adverse effects on their credit could limit their ability to meet key financial goals like purchasing a home or even obtaining employment.10

These facts are not lost on younger consumers. As early adopters of financial technology such as peer-to-peer (P2P) payments, cryptocurrency, and investing apps, they were among the first affected by spectacular digital security failures. For example, scams targeting P2P payment users have been rampant since the inception of these services and complaints of these scams surged 300% in 2021.11 High-flying cryptocurrency exchanges have experienced a seemingly nonstop series of security compromises, resulting in millions of dollars lost to criminals.12 Even a popular trading app — whose median user age is 31 — saw a string of account takeovers that left investors wondering when, or even if, they could ever be made financially whole.13,14

Considering the security risks that exist in today’s digital-heavy financial environment, it only follows that identity safety is critical to younger consumers’ financial health — both real and perceived. Yet, for all that has been invested by financial institutions in account security and consumer identity safety, none of it delivers a special, personalized experience for the ultimate user. Which is why none of those technology investments have had the ability to attract and retain younger consumers — at least, not yet.

10 Identity Theft Resource Center (ITRC), Identity Theft: The Aftermath Study, 2021
11 Fortune, There Are New Scams on Mobile Payment Apps—And Teens Aren’t Immune, 2021
12 Federal Trade Commission, Cryptocurrency Buzz Drives Record Investment Scam Losses, 2021
13 CNBC, Fintech-App Robinhood is Driving a Retail Trading Renaissance During the Stock Market’s Wild Ride, 2020
14 Mish Talk, Robinhood Accounts Looted and No Customer Service to Call, 2020
CREDIT SCORES ARE NOT IDENTITY SAFETY

A popular feature of digital banking, free credit tools don’t necessarily offer younger consumers a complete picture of their risk exposure. Aspects of credit monitoring, like credit scores, are clearly personalized. Yet the credit profiles of Gen Z consumers and even millennials are still in the early stages of maturation. There is less to monitor and therefore they may be less inclined to use these tools. Instead, they are likely more actively engaged in investing, saving and transacting online. While each of those areas are being targeted by fraudsters and scammers, credit scores alone are often insufficient to identify fraud on accounts that already exist.

With so much financial data living within digital channels heavily targeted by bad actors, broad-based identity safety is an undeniable necessity for true financial health among digital-native younger consumers.

Credit monitoring has proven how much consumers value personalized and action-oriented scores, and yet the audience for personalized identity safety scores is even broader. Empowering them with personalized solutions to protect the entirety of their financial lives is exactly the kind of differentiation that can win the loyalty of Gen Z consumers and millennials alike — not to mention older and more affluent ones.

The personalized identity insights and actionability Sontiq provides can make the winning difference, delivering greater value and utility to younger consumers. There was a six-percentage point difference favoring Sontiq’s BreachIQ™ over credit monitoring by financial services consumers under the age of 35.15 And even more, Sontiq can enhance the value of investments in free credit tools and popular account controls to better meet the needs and expectations of these consumers.

15 BreachClarity, 2020 online survey of 1,000 U.S. adults, 2020
PERSONALIZING IDENTITY SAFETY

When it comes to maintaining both the trust of consumers and the financial strength of financial institutions, the importance of account safety cannot be overestimated. Collectively, financial institutions invest billions in controls and processes designed to keep accounts secure, which includes deploying a variety of consumer-facing controls. But lackluster adoption rates mean that these controls have underperformed when compared to their promised ROI. When consumers do engage, it often leads to additional costs by way of increased call volume (more on that later). It is only through personalization that financial institutions can truly drive better security behaviors, with the added benefit of empowering consumers to safeguard their financial health.

Today financial institutions deploy a range of consumer-facing tools to help manage the risk of everything from card fraud to account takeover. Alerts and notifications cover any number of account and transaction events, but rarely offer security benefits to consumers beyond a look at unusual card transactions. And, despite widespread availability, the actual use of card controls has been of little interest to most cardholders.

Of course, these challenges and frustrations are felt beyond a financial institution’s virtual walls. Even Google has complained that adoption of two-factor authentication is far too low at only 10%, which is clearly an issue when email accounts like Gmail are the destination for many account alerts and password reset schemes. (To enhance security, Google announced in May 2021 that it would require two-factor authentication by default.) Basic password hygiene is so overlooked that the results of annual studies on the most common passwords change little from year to year. The list of poor practices is long. And considering the digital orientation of younger consumers, the risks posed to them and their financial service providers by these identity safety missteps are amplified greatly.

Long before fraud even occurs, financial institutions can be subjected to the costs created by consumers’ growing anxiety around data breaches. Half of all younger consumers who have experienced a data breach have contacted their financial institution for assistance at least once (see Figure 2). To provide such assistance, institutions can spend up to $5 in call-center support per instance, in addition to the expenses they have for chat, text and email assistance. Unfortunately, without the ability to provide personalized recommendations in the wake of a breach, those investments can only provide the kind of generic advice that (as illustrated above) younger consumers value less.

FIGURE 2:
In Search of Answers, Data Breaches Drive Calls to Financial Institutions for Consumers of All Ages

| Breach Victims Who Contacted Their Financial Institution, by Age |
|-------------------|---|---|---|
|                    | Under 35 | 35–54 | 55+ |
| 60%                | 50%       | 48%   | 44% |
| 50%                | 40%       | 30%   | 20% |
| 40%                | 30%       | 20%   | 10% |
| 30%                | 20%       | 10%   | 0%  |
| 20%                | 10%       | 0%    | 0%  |
| 10%                | 0%        | 0%    | 0%  |
| 0%                 | 0%        | 0%    | 0%  |

SOURCE | BreachClarity online survey of 1,000 U.S. adults, May 2020

16 The Verge, Google is About to Turn on Two-factor Authentication by Default for Millions of Users, 2021
17 CX Today, How to Calculate Your Cost per Inbound/Outbound Call and Why?, 2021
Digital channels have been transformative for financial services, reimagining costly services from other channels and making them easier to use and more convenient. Although the digital arena is one where some financial institutions have historically been at a disadvantage, leveraging Sontiq's BreachIQ in digital channels applies a transformative effect to the massive problem of data breaches. By delivering risk scores and identity safety scores, highlighting breach risks and prioritizing personalized action steps for the consumer, BreachIQ moves account holders out of the call center and into an engaging digital experience. It offers consumers proactive identity safety insights, guidance and peace of mind. Further still, Sontiq places the very actions that some institutions have struggled to get consumers to use right at their fingertips, just when they need it most.

Sontiq’s technology is a simple and cost-effective — yet sophisticated — approach for improving financial wellness, improving trust and delivering the type of digital experience that younger consumers want from their financial service provider. It speaks directly to the younger generation, empowering them to tackle the often-overwhelming identity security problem and ensuring that they have the same opportunity to achieve financial health goals as the generations that came before them. Regardless of size, any financial institution can show them the way.

To learn more about how Sontiq can deliver the standout personalized insights and digital engagement that Gen Z and millennial consumers expect, visit us at www.sontiq.com or request a demo at sontiq.com/partnerships/schedule-a-demo.

ABOUT SONTIQ

Sontiq, a TransUnion company, is an intelligent identity security company arming businesses and consumers with a full range of award-winning identity and cyber monitoring solutions, as well as best-in-class restoration and response offerings. Sontiq products empower millions of customers and organizations to be less vulnerable to the financial and emotional consequences of identity theft and cybercrimes. Sontiq has an outstanding track record for delivering high-touch support and fraud remediation services, demonstrated through its 99% customer satisfaction ratings. https://www.sontiq.com