

ANONYOME LABS



Digital Identity Protection:

A Bank's Path to New Revenue and Become a Cyber Safety Hero

As a bank, you hold a crucial position to be one of your customers' most trusted organizations. Providing digital identity protection tools is an excellent opportunity to add a new revenue stream and protect your customers.

According to an Experian study, financial institutions rank as the third most trusted businesses among consumers. While you already invest considerable effort in securing your customers' accounts and funds, there's an opportunity to extend the same level of protection to their digital identities.

Here is the opportunity: 50% of consumers feel that they wouldn't know where to begin when it comes to protecting themselves from identity theft and cybercrime. This eBook takes an in-depth look at the current fraud and privacy threats confronting bank customers and how you can solve your customer's problem.



We'll cover:

What banks are doing/can do to keep their customers safe within their organization:

- Staff Training
- Account onboarding/KYC screening
- Adding New Technology

What banks can do for their customers outside their organization:

- Credit and Identity Theft Monitoring
- Cyber Safety (password manager, virtual private network, virtual cards, secure ID, verification)
- Secure Communications (encrypted voice, video, email, and messaging)
- Open Communications (phone numbers, SMS/MMS messaging, voice calling, email)
- Safe Browsing (private browser, ad, and tracker blocker, site reputation service)

Here's everything you need to know to keep your customers safe with all their online interactions and creating a new revenue stream with digital identity protection tools.



The 7 Reasons Why and How Banks Should Offer Identity Protection Products

Banks play a crucial role in protecting their customers in today's digital age, where personal information is always at risk. Offering identity protection products goes beyond a service—it's a commitment to the security and well-being of each customer.

Here's why and how banks should integrate identity protection into their offerings:



1. Customer Trust and Assurance:

Why it matters: Customers trust their banks to prioritize their financial well-being.

How to achieve it: By expanding their protective measures beyond financial transactions, banks can cultivate trust and demonstrate their dedication to customer security.



2. Evolving Customer Expectations:

Why it matters: Consumer expectations rapidly change, demanding comprehensive security measures.

How to achieve it: Banks can stay ahead of these expectations by providing robust identity protection that meets current needs and gains a competitive edge in the market.



3. Addressing the Privacy Paradox:

Why it matters: The privacy paradox—where individuals express concern about privacy but still engage in risky online behaviors—underscores the need for proactive protection.

How to achieve it: Banks can address this paradox by offering educational resources alongside identity protection, empowering customers to make informed decisions about their digital security.



4. Mitigating Digital Fraud:

Why it matters: The complicated landscape of digital fraud creates constant threats to personal information.

How to achieve it: Banks can protect customers against various types of fraud by providing them with comprehensive tools and resources that identify, treat, and prevent cyber threats.



5. Enhancing Customer Loyalty:

Why it matters: Customers who feel secure and supported will stay loyal to their banks.

How to achieve it: By offering identity protection, banks enhance customer loyalty and create a valuable point of differentiation in a crowded financial services landscape.



6. Streamlining Security Solutions:

Why it matters: The complexity of adopting multiple security solutions can overwhelm customers.

How to achieve it: Banks simplify customers' lives by consolidating various digital protection measures into a user-friendly offering, ensuring ease of use and effectiveness.



7. Diversifying Revenue Streams:

Why it matters: Identity protection can serve as a valuable revenue stream for banks.

How to achieve it: By strategically integrating identity protection into their service lineup, banks not only enhance security but also unlock new opportunities for revenue generation.

In conclusion, banks can position themselves as the guardians of their customers' digital lives by offering identity protection. Beyond being a service, it becomes a testament to the bank's unwavering commitment to customer security, trust, and overall financial well-being.

Why Your Customers Need Identity Help: The Privacy Paradox



According to the ID Theft and Cybercrime Research report, 50% of consumers admitted needing help with safeguarding themselves from identity theft and cybercrime.

Moreover, 84% of customers agreed that there are crucial measures to protect themselves from identity theft or cybercrime that they cannot undertake independently.

This brings us to the Privacy Paradox.

Privacy Paradox: When people are very concerned about their privacy while not taking action to protect themselves.

The Privacy Paradox refers to the gap between people's stated value of privacy, as seen in surveys and behavioral studies, and their actions regarding their digital identity. This paradox is not a random statistical phenomenon but is influenced by complex factors that affect people's decision-making process.

One reason why people expose their digital identity is because security often comes at the cost of convenience. The desire for social connection, the feeling of anonymity, and the perceived benefits of sharing personal information are some factors shaping these decisions. However, consumers have expressed their concerns about identity theft (64%), stolen credit card information (61%), and online privacy (60%) as top issues when conducting online activities, according to Experian.

The Privacy Paradox is a problem that banks can solve. Here's the stats:

- Over 60% of consumers would purchase identity theft and cyber protection.
- 37% of consumers wish their financial institution offered identity protection.

You become a trusted partner in their journey by offering valuable solutions that address customers' needs. Elevate their experience, build trust, and create another revenue stream by providing the support and resources they need to protect themselves in the digital world.

Digital Identity Super-Villains: Unmasking the Threats

You already know how far fraudsters will take advantage of a situation. Over 66% of financial institutions have over half of their employees working on fraud-related projects and activities.

So, we'll do a quick overview:

Villain 1: Dr. Darknet

Alias: The Dark Web Overlord

Dr. Darknet thrives in the shadows of the internet, orchestrating a network of cybercrime that spans the mysterious realm of the dark web. Armed with anonymity, this villain trades in stolen digital identities, financial information, and more.

Bank customers must guard against Dr. Darknet's schemes to protect their online presence.



Villain 2: Master Manipulator

Alias: The Social Engineer

Known as the Master Manipulator, this villain preys on the vulnerabilities of human psychology. Armed with cunning tactics, persuasive charm, and a knack for deception, the Social Engineer tricks individuals into revealing sensitive information.

Bank customers must stay vigilant against this adversary's schemes, recognizing the signs of manipulation to safeguard their identities.



Villain 3: Phisherman

Alias: The Deceptive Angler

Phisherman is a cunning villain who casts deceptive lures across the digital seas, attempting to reel in unsuspecting victims. This adversary tricks individuals into giving confidential information through fraudulent emails, messages, or websites.

Bank customers must sharpen their phishing detection skills to avoid falling into Phisherman's traps and protect their digital identities.



Villain 4: Identity Impersonator

Alias: The Mimic

The Identity Impersonator excels in assuming the digital personas of unsuspecting individuals. This villain utilizes stolen information to impersonate others, leading to fraudulent activities and potential financial loss.

Bank customers must guard against The Mimic's attempts to masquerade as them in the digital realm.





These digital identity super villains represent the formidable adversaries banks' customers face in the ever-evolving cybersecurity world.

To protect themselves against villains,



Recommends that
your customers:

- Explore security tools
- Use multi-factor authentication
- Clear their cache regularly
- Use different email addresses for various kinds of accounts
- Use a password manager to have unique passwords for every login
- And many more safety measures.

The long list of what your customers "should" be doing becomes incredibly overwhelming, and it is hard to start the process independently. This is where your banks comes in to save the day.

What Banks Can Do to Protect Customers Outside Your Organization



As one of the most trusted institutions for its customers, a bank is uniquely positioned to package many necessary solutions into a single, effective, and easy-to-use digital identity protection offering.

A Javelin Strategy & Research study found that offering identity protection services led to increased trust among banking customers, resulting in higher satisfaction and loyalty rates.

Add to that the inherent behavior change that comes with identity protection becoming convenient, and you've just rescued your customers from the deadly clutches of the privacy paradox.

Here are some digital identity protection services you could package and offer to your customers:

- 1 Credit and Identity Theft Monitoring:** Regular three-bureau credit reporting, locking mechanisms, and vigilant monitoring with instant alerts to counteract identity theft.
- 2 Online Footprint Analysis and Cleanup:** Empower customers to uncover entities holding their Personally Identifiable Information (PII). You can show them an easily navigated path to cleaning up their online presence and invoking the "right to be forgotten." 57% of consumers said they would be willing to pay for the ability or service to view and delete the personal data companies collect. -Deloitte's Digital Media Trends survey.

- 3 Safe and Private Browsing:** Equip customers with robust tools for secure, private digital experiences. This includes a mobile private browser, desktop safe browsing extension, ad and tracker blocking, and site reputation services.

Only about 25% of internet users in the United States use ad blockers. - Statista

- 4 Virtual Private Network (VPN):** Provide customers with a secure and private internet connection, stop online tracking, data exposure, and other online risks.

- 5 Password Management:** Simplify the protection of online interactions by enabling customers to create, store, and manage secure login credentials across all their online services, guarding against weak or exposed passwords.

69% of Americans feel overwhelmed by the number of passwords they have to keep track of, and nearly half (46%) will create passwords that are easier to remember, even if they are less secure. - Pew Research

- 6 Separate Identity Spaces:** Give customers complete control over their online identity. By creating unique email and phone numbers, they can protect themselves across their interactions. For instance, customers can have an extra layer of security for specific purposes such as shopping, social media, travel, dating, gaming, and more.

How Banks Protect Their Customers Internally

You work incredibly hard to protect your customers internally by staff training, improving processes like KYC, and implementing new and better technology.

Staff Training:

You can reinforce your defenses against fraud with targeted staff training.

These initiatives could include:

- Cybersecurity awareness programs
- Simulated phishing exercises
- Clear data protection protocols
- Incident response drills
- Compliance and regulatory training

By investing in the knowledge and vigilance of their teams, banks bolster internal defenses and fortify the security of customer data.

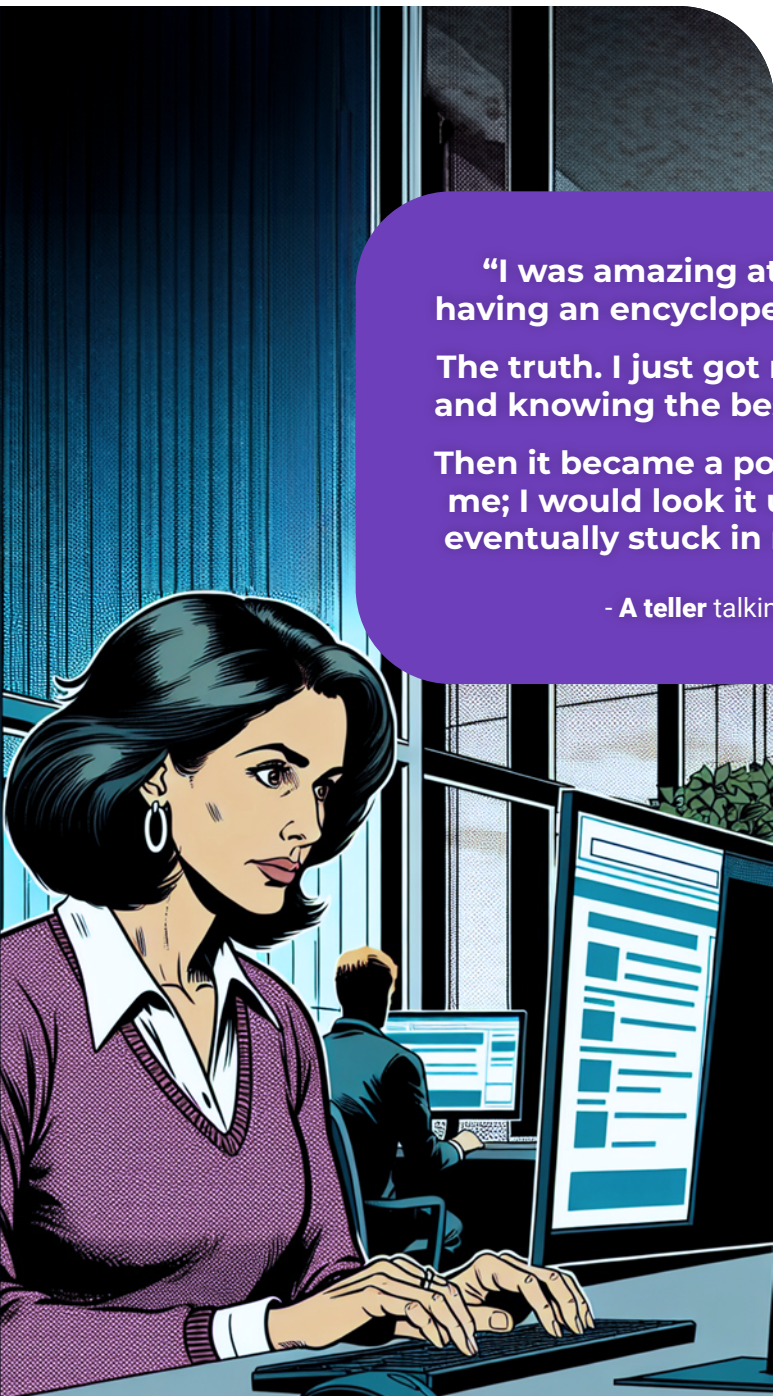
“I was amazing at my job in the branches and known for having an encyclopedia in my head on banking regs and laws. The truth. I just got really good at learning our internal guides and knowing the best sites to look stuff up (google can be iffy). Then it became a positive feedback loop. Folks would come to me; I would look it up quickly and give an answer. Some of it eventually stuck in my brain so I wouldn't have to look it up.”

- A teller talking about their experience on an online forum. -

Robust Know Your Customer (KYC): By creating thorough and precise identity verification processes during onboarding and transactions, you significantly lower the risk of fraud. Some FIs can experience up to 40% of attempts to open accounts are fraudulent.

Add New Technology: Technological solutions complement your other efforts with advanced authentication measures, encryption protocols, and secure communication channels.

With the right tools, individuals and organizations can better equip themselves against the evolving strategies employed by malicious entities.





Empower Your Customers: Seamless Digital Identity Protection

Offering robust digital identity protection for your customers has never been easier, thanks to Anonymome Labs. We simplify the process, enabling you to effortlessly provide a suite of digital identity protection.

Our digital identity protection components:

- **Password Manager:** Enhance online security with a tool that ensures unique and robust passwords for every login.
- **Virtual Private Network (VPN):** Provide a secure and private internet connection, shielding customers from online risks.
- **Private Browser:** Enable secure and private online experiences with dedicated mobile and desktop browsers.
- **Ad and Tracker Blocker:** Shield customers from intrusive ads and trackers, preserving their online privacy.
- **Site Reputation Service:** Keep customers informed about the trustworthiness of websites they interact with online.
- **Encrypted Communication:** Ensure privacy across voice, video, email, and messaging platforms with cutting-edge encryption.
- **Open Communications:** Provide customers with secure and private phone numbers, SMS/MMS messaging, voice calls, and emails to safeguard their personal contact information.

About Our Business

Anyome Labs, a trailblazer in privacy and identity protection since 2014, has worked with leading companies across industries. Our digital identity protection tools, coupled with services like credit monitoring, antivirus, and identity theft insurance, have empowered over 150,000 consumers.

Your customers could be the next people to have peace of mind from seamless digital identity protection.

Anyome Labs has everything necessary to create a digital identity protection suite that:

- You can tailor the offering to meet the unique needs of your customers.
- Can be built into your existing apps, interfaces, and systems (or as a hosted solution).
- You can “Make it your own” with your branding, colors, and logo.



Be your customer's hero - connect with our team today to explore the impact that our Digital Identity Protection tools can have!



ANONYOME LABS