



PYMNTS®

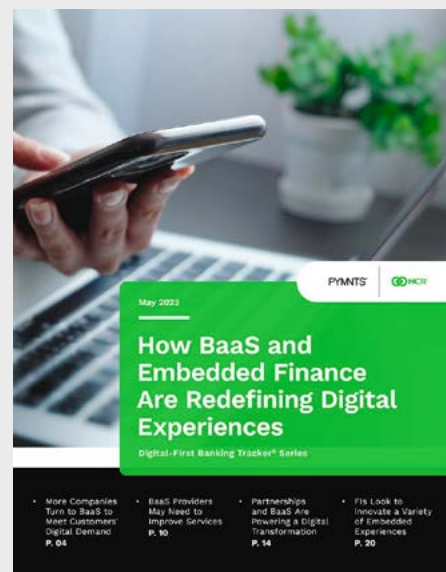


MAY/JUNE 2023

# Stopping Bank Fraud With Cybersecurity Solutions

Digital-First Banking Tracker® Series

■ Read the previous edition



MAY 2023

Digital-First Banking Tracker® Series

- Fraud's Impact on the Banking and Financial Industries  
**P. 04**
- Most Consumers Trust Banks to Keep Credentials Secure  
**P. 10**
- The Best Anti-Fraud Solutions for Banks and Their Customers  
**P. 14**
- Payment Security Market to Exceed \$64B by 2030  
**P. 26**

# What's Inside

## 04 Fraud's Impact on Consumers and Banks

Four in 10 individuals have had their personal information stolen or compromised in the past year.

## 10 Most Consumers Trust Banks to Keep Credentials Secure

More than 58% of consumers say they trust their primary banks to vault their payment credentials.

## 14 The Best Anti-Fraud Solutions for Banks and Their Customers

PYMNTS details the most effective solutions banks can leverage to prevent cybercrime and its associated lost revenue.

## 20 Security Is Key Driver of Customers' Trust in Financial Service Providers

Eighty-two percent of customers said that having at least one security feature was very or extremely impactful on their trust in a financial service provider.

## 22 Combating the Rising Tide of CNP Fraud

PYMNTS interviews Kevin Lambrix, senior vice president and merchant acquiring risk leader at KeyBank, about responding to the uptick in card-not-present fraud as criminals seek the path of least resistance.

## 26 Payment Security Market to Exceed \$64B by 2030

An increase in fraud levels is the biggest contributor to this growth, and security providers have rolled out new technologies to combat it.

## 28 About

Information on PYMNTS and NCR

PYMNTS®



### Acknowledgment

The Digital-First Banking Tracker® Series is produced in collaboration with NCR, and PYMNTS is grateful for the company's support and insight. PYMNTS retains full editorial control over the following findings, methodology and data analysis.



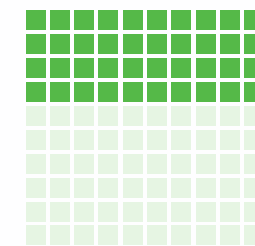
## Need to Know

# Fraud's Impact on Consumers Is Significant

A substantial number of Americans can expect to [experience digital fraud](#) at least once in their lifetime, with a recent study finding that four in 10 individuals have had their personal information stolen or compromised in the past year. Fifty-one percent of these victims lost personal funds when their accounts were compromised, and half of victims said they were targeted more than once.

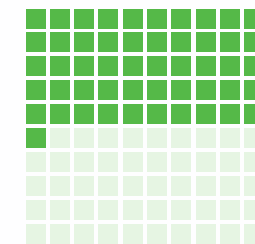
Fraud that exploits individual consumers takes on a wide variety of forms: 72% of Americans have received a [text or direct message](#) that they thought was part of a scam, and 43% say a friend or family member has fallen victim to a similar scam. Account takeovers, identity theft and social engineering are just some of the methods bad actors use to defraud their victims.

Fraud affects countless individuals every year.



**40%**

Portion of Americans who have had their personal information stolen or compromised in the past year



**51%**

Share of fraud victims who lost personal funds

## Need to Know

# Fraud takes a heavy toll on the banking and financial industries.

Fraud's impact on banks and other financial organizations mirrors its effect on consumers, with [46% of organizations](#) in a recent survey saying they had experienced fraud in the past two years. Among organizations making more than \$10 billion a year, 52% experienced fraud, and one in five of these said their fraud cost more than \$50 million.

Fraud aimed at financial institutions (FIs) has become increasingly sophisticated, with attackers frequently leveraging botnets and other advanced technologies in their schemes. PYMNTS research found that one-quarter of large FIs reported this [increasing fraud sophistication](#) to be their single biggest challenge.

**Fraud affects organizations as much as it does consumers.**



**46%**

**Portion of businesses that have experienced fraud in the past two years**



**\$50M**

**Amount lost to fraud by one in five businesses making more than \$10 billion annually**

## Need to Know

# Anti-fraud solutions are key to keeping FIs and their customers safe from cybercrime.

According to a recent PYMNTS study, 71% of large FIs plan to initiate or improve solutions using artificial intelligence (AI) or machine learning (ML) to combat fraud and financial crimes. Among smaller FIs, the percentages are lower, ranging from 27% to 65%, depending on asset size.

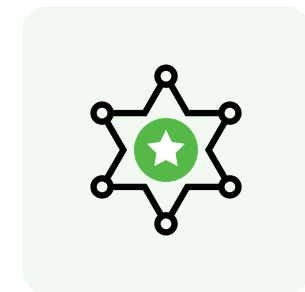
AI and ML are some of the most promising cybersecurity tools available for recognizing consumer patterns and identifying deviations that could be signs of fraud. While cybercrime may never be stopped completely, solutions such as these could offer a meaningful reduction in fraud's impact in the coming years.

**Banks are highly concerned about the impact of fraud on themselves and their customers.**



## 25%

Share of FIs with \$500 billion or more in assets that perceive fraud's new sophistication as their most important challenge



## 95%

Portion of anti-money laundering executives who highly prioritize innovative fraud-fighting solutions



## News and Trends

---

# Most Consumers Trust Banks to Keep Credentials Secure

A recent PYMNTS survey found that while consumers are well aware of the risks of fraud, they generally trust their banks to keep them safe from bad actors. More than 58% of consumers said they would entrust their primary banks with vaulting their payment credentials, while smaller shares expressed confidence in payment providers or eCommerce merchants such as PayPal, Amazon or Apple to do the same.

The study further found that 60% of consumers store payment credentials with various businesses rather than entering them each time. Fifty-one percent of consumers expressed interest in a third-party vault to keep credentials secure rather than storing this data with individual banks or merchants.



## News and Trends

### Identity fraud cost banks a median of \$310K last year

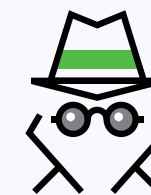
Identity fraud is a particularly dangerous threat to the banking sector, with a recent study finding that the median loss per bank last year clocked in at \$310,000. Nearly one-third of banks lost \$497,000 or more during the same time period, while FinTechs lost a median of only \$120,000. The median across all surveyed sectors, including aviation, technology, telecommunications and financial services, was \$240,000.

Banks' greater share of losses may reflect their larger scale and complexity as well as their unique regulatory risks compared to FinTechs. In support of this conclusion, while business disruption was the leading source of costs for all organizations, followed by legal costs, banks' second-largest cost due to identity fraud consisted of penalties and fines.

### AARP: Identity fraud cost Americans \$43B last year

Educating consumers about the dangers of identity fraud appears to be having an impact, though the crime still represents a major threat. A recent study sponsored by the American Association of Retired Persons (AARP) found that while identity fraud cost Americans \$43 billion in 2022, this was down \$9 billion from the year before. Both traditional identity fraud via data breaches and fraud via scams in which individuals were tricked into divulging information were measured.

The study's authors attributed this decline to consumer outreach and increasing individual awareness of scam methods. Scams made up the bulk of identity fraud cases, affecting 25 million victims and causing \$23 billion in losses, down \$5 billion from 2021.



# \$43B

**Total identity fraud costs in U.S. in 2022**



# \$23B

**Losses due to identity scams in U.S. in 2022**



## PYMNTS Intelligence

---

# The Best Anti-Fraud Solutions for Banks and Their Customers

Fraud's cost goes far beyond the actual amount stolen, with a recent study finding that every dollar lost to fraud costs FIs approximately \$4.36 in total. Moreover, this represents only directly related expenses, such as legal fees and recovery: The [true cost of fraud](#), taking lost customer loyalty into account, is likely incalculable.

Fraud-fighting solutions may be expensive, but they more than pay their freight when considering this cost. This month's PYMNTS Intelligence details the most effective solutions banks can leverage to prevent cybercrime and its associated lost revenue.





## PYMNTS Intelligence

### Balancing security with convenience

While 74% of customers value good [fraud protection as a top-three consideration](#) when applying for financial accounts, 25% say they have abandoned a checking account application due to obtrusive authentication procedures. A customer lost to friction is just as gone as one lost to bank fraud, so banks must walk a fine line in balancing the competing needs for security and convenience.

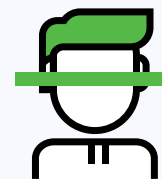
One of the most effective ways to authenticate customers seamlessly yet securely is with [biometrics](#), which offers excellent protection and is favored by large portions of customers. More than 36% of customers prefer to use fingerprint scans for authentication, while 34% favor facial recognition technology.

Consumers enjoy using biometric verification both for its security and for its seamlessness.



**36%**

Portion of consumers who prefer to use fingerprint scans for authentication



**34%**

Share of consumers who prefer to use facial recognition technology

Businesses of all types, including banks, are [adopting biometrics](#) in record numbers to counter the rising threat of digital fraud. Fifty-six percent of businesses worldwide that leverage document verification tools offer facial recognition, and 91% plan to increase their spending on identity verification processes in the next three years. Partnering with third-party vendors is one way to fast-track implementation of fraud prevention procedures.

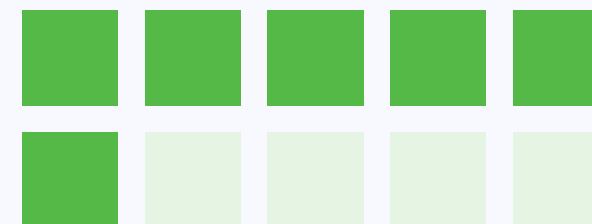
## PYMNTS Intelligence



## The value of partnerships in bolstering cybersecurity

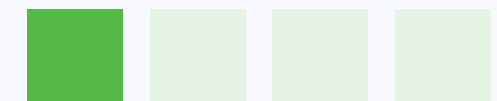
Some advanced biometric security measures are expensive to implement, especially for smaller FIs that lack a dedicated in-house biometrics team. One survey of bank executives found that 70% lack the data analysis and AI capabilities to compete long-term with banks that have the resources to develop in-house security technology.

Third-party partnerships are a critical resource for covering these knowledge gaps, as they offer plug-and-play solutions that fight fraud and verify consumers' identities without the need for in-house expertise. Six in 10 banks plan to increase their IT spending on fraud management in 2023, and third-party verification solutions could be an especially high-value investment.



### 6 in 10

Portion of banks  
increasing their IT spend  
on fraud management



### 1 in 4

Share of banks that plan to  
increase fraud management  
spending by 6% or more



Chart of the Month

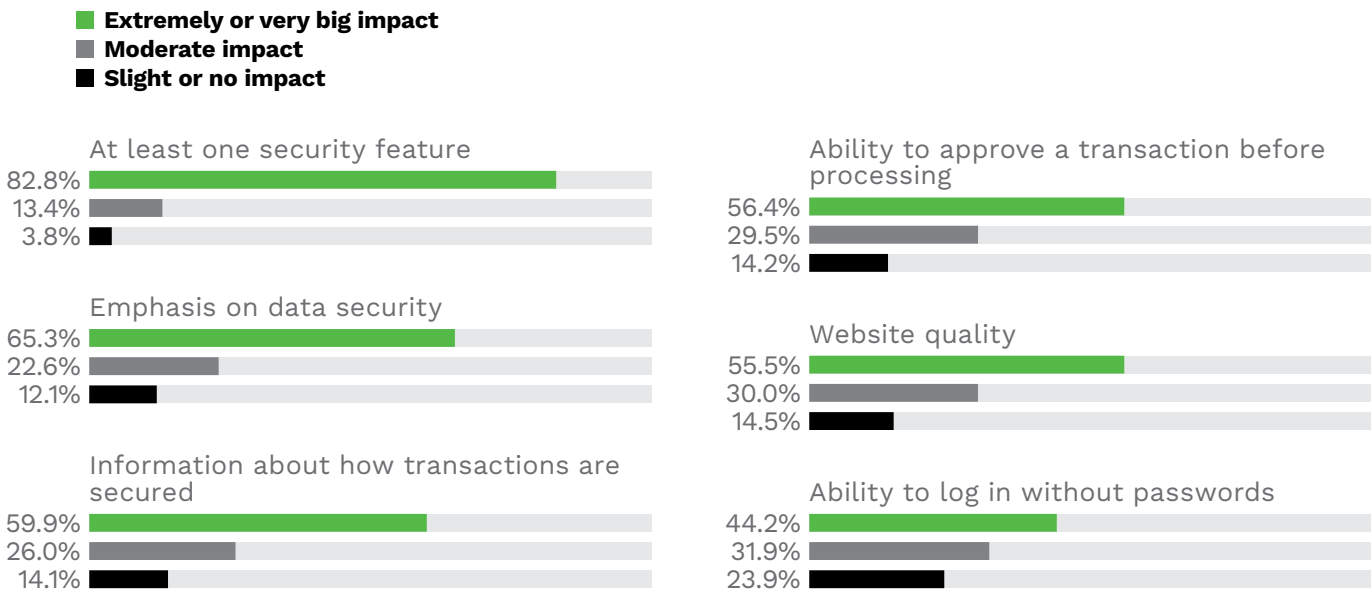
# Security Is Key Driver of Customers’ Trust in Financial Service Providers

Bank customers place a great deal of trust in their financial service providers to keep their money safe from fraud, financial hardship and bad business decisions. In fact, a recent PYMNTS study found that security was the top driver of customer trust. Eighty-three percent of customers said that having at least one security feature was very or extremely impactful on their trust in a financial service provider, and 65% said an emphasis on data security was extremely important. In addition, 60% of respondents said that information about how transactions are secured was extremely impactful on their trust.



### What builds trust in financial service providers

Share of consumers who cite select factors as very or extremely impactful on their trust in a financial service provider



Source: PYMNTS  
Finding the Balance Between Security and Convenience, June 2022  
N = 2,719: Complete responses, fielded March 23, 2022 – April 1, 2022

## Insider POV

# Combating the Rising Tide of CNP Fraud



**KEVIN LAMBRIX**

Senior vice president and  
merchant acquiring risk leader



“The criminals, they’re very adept at figuring out ways around people’s best defenses. So we constantly have to anticipate and try [to] mitigate what we think could happen on top of what we know will happen.”

PYMNTS interviews Kevin Lambrix, senior vice president and merchant acquiring risk leader at [KeyBank](#), about the competing factors that limit measures against card-not-present (CNP) fraud and what can be done about them.

Card-present security features such as EMV chips have [pushed fraud toward CNP transactions](#), and consumer eCommerce demand is fueling that growth. Larger and more sophisticated eCommerce players are reasonably effective at combating CNP fraud, Lambrix told PYMNTS, but newer players are often underprepared to meet the security challenges. While businesses take fraud more seriously once they have been burned, the rush to get a product to market and the assumption that turnkey platforms have fraud prevention baked in can leave novices vulnerable.



## Insider POV

---

**Security protocols such as 3D Secure are valuable only if they are implemented, and that may require regulatory involvement.** In the United States, there are currently no requirements to implement 3D Secure, a protocol that makes it more difficult to commit CNP fraud, Lambrix said. Merchants are left to weigh the cost of implementation against the immediate benefits to themselves. Often the potential losses from fraud — at least from the merchant's perspective — are of less concern than the potential losses from being unable to run less secure transactions.

**It will take a mixture of education and the right tools— for consumers as well as businesses — to keep ahead of CNP fraud.** Lambrix said the industry has yet to come together to implement CNP fraud standards because different solutions may fit better for different situations. On the other hand, businesses are also inherently motivated by revenue, and if a solution will reduce their fraud exposure in a way that makes fiscal sense, they will be interested. Getting there is a matter of helping companies understand the available tools and how they can benefit from them.





## What's Next

---

# Payment Security Market to Exceed \$64B by 2030

Financial security's importance in the eyes of both consumers and banks means that FIs will pay top dollar for it. A recent study found that the payment security market's value is poised to cross the \$64-billion mark by 2030, rising at a compound annual growth rate of 14% over the next seven years. An increase in fraud levels is the biggest contributor to this growth, the study found, with security providers rolling out new technologies to combat it. Mobile security will be a particular value driver in the coming years as more consumers bank and transact from their smartphone devices, which will need to be secured just as well as web-based banking and brick-and-mortar branches.

“There's no single way that FIs can protect themselves from the evolution of fraud. Bad actors come from all angles, so FIs need to use all the tools at their disposal, including advanced data analytics, behavioral biometrics, real-time monitoring and alerts, information sharing with partners and peer banks and then, of course, customer education. Banks and credit unions have to take a multilayered approach to stay one step ahead of future fraudsters and attacks.”


**DOUG BROWN**  
President





# About

**PYMNTS®** **PYMNTS** is where the best minds and the best content meet on the web to learn about “What’s Next” in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

 **NCR Corporation** is a leader in banking and commerce solutions, powering incredible experiences that make life easier. With its software, hardware and portfolio of services, NCR enables transactions across financial, retail, hospitality, travel, telecom and technology industries. NCR is headquartered in Atlanta, Georgia, with 34,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at [feedback@pymnts.com](mailto:feedback@pymnts.com).

# Disclaimer

The Digital-First Banking Tracker® Series may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED “AS IS” AND ON AN “AS AVAILABLE” BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS is the property of PYMNTS and cannot be reproduced without its prior written permission.

The Digital-First Banking Tracker® Series is a registered trademark of What’s Next Media & Analytics, LLC (“PYMNTS”).