FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i VIPPS MOBILEPAY AS
Postboks 9236 Grønland
0134 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
23/9268			15.04.2024

Tilsynsrapport

Finanstilsynet gjennomførte IKT-tilsyn i Vipps MobilePay AS (Vipps) 24. og 25. oktober 2023. Tema for tilsynet var å vurdere Vipps' etterlevelse av bestemmelser om styring og kontroll med drift og beredskap med krav i IKT-forskriften og finansforetaksforskriften § 3-2, samt med øvrige krav i finansforetaksforskriften § 3-2. Tilsynet var begrenset til den norske virksomheten.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 19. januar 2024 og styrets kommentarer til rapporten i brev av 25. februar 2024.

Finanstilsynet har følgende merknader etter tilsynet:

Overordnet styring og kontroll

Finansforetaksloven § 13-5 stiller krav til forsvarlig virksomhet og god forretningsskikk. Foretaket skal ha klare og hensiktsmessige styrings- og kontrollsystemer samt hensiktsmessige retningslinjer og rutiner for å styre, overvåke, og rapportere risiko foretaket er, eller kan bli eksponert for, jf. finansforetaksloven § 13-5 første ledd. I henhold til § 13-5 annet ledd skal foretaket ha uavhengige kontrollfunksjoner med ansvar for internrevisjon, risikostyring og etterlevelse av krav fastsatt i eller i medhold av lov eller forskrift. Foretaket faller inn under unntaket om krav om internrevisjon, jf. finansforetaksforskriften § 8-3 første ledd, og har ikke etablert internrevisjon.

Internkontrollaktiviteter i første- og andre forsvarslinje

Finanstilsynet pekte i foreløpig rapport på at Finanstilsynet forutsatte at første forsvarslinje definerer og utfører egne internkontroll-aktiviteter inkludert for anthvitvasking og -terrorfinansiering, samt for IKT-sikkerhet, uavhengig av andre forsvarslinje.

Fra styrets svar har Finanstilsynet merket seg at styret tar innspillet fra Finanstilsynet til etterretning og vil påse at rollefordelingen mellom første- og andrelinjen når det gjelder internkontroll-aktiviteter tydeliggjøres og presiseres enda bedre i foretakets rammeverk for risikostyring og internkontroll. Det presiseres at første forsvarslinje eier risikoene og er ansvarlig for utføring, dokumentasjon og egenevaluering av internkontroll-aktivitetene, mens andre forsvarslinje er ansvarlig for å legge til rette for en risikobasert og virksomhetsinnrettet internkontroll i form av standarder og verktøy som skal sikre effektive, standardiserte og systematiske internkontroll-prosesser.

Finanstilsynet tar styrets svar til etterretning.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Åshild Johnsen
Dir. tlf. 22 93 97 02

Sikre uavhengige tredjepartsvurderinger
Den tredje forsvarslinjen i Vipps består av eksternrevisors årlige uavhengige bekreftelse til styret om risikostyring og internkontroll i selskapet. Vipps faller inn under unntaket om krav om internrevisjon, jf. finansforetaksforskriften § 8-3 første ledd og har ikke etablert internrevisjon.

Finanstilsynet viste i foreløpig rapport til at Vipps som tilbyder av betalingstjenester, som de fleste privatpersoner og stadig flere bedrifter baserer seg på, har vokst til en betydelig virksomhet med mange ansatte og stor omsetning. Etter Finanstilsynets vurdering bør Vipps rutinemessig bestille uavhengige tredjepartsvurderinger, og det bør etableres en rutine som beskriver hva som skal ligge til grunn for valg av temaer samt sikrer at uavhengige tredjepartsvurderinger blir gjennomført. Finanstilsynet ba videre styret vurdere å etablere internrevisjon.

Finanstilsynet har merket seg at styret tar innspillet fra Finanstilsynet til etterretning og at det bekrefter at det skal etableres en standard/rutine for valg av temaer for og gjennomføring av uavhengige tredjepartsvurderinger. Finanstilsynet har videre merket seg fra styrets svarbrev at Vipps fortløpende skal vurdere behovet for å etablere en internrevisjonsfunksjon.

Finanstilsynet tar styrets svar til etterretning.

Drift og beredskap
Ifølge IKT-forskriften § 8 første ledd skal driften av IKT-virksomhet være basert på dokumenterte prosedyrer. Prosedyrene skal sikre fullstendig, rettidig og korrekt behandling og oppbevaring av data. Foretaket skal ha dokumenterte driftsløsninger for IKT-virksomheten. Driftsløsningene skal sikre tilgjengelighet i tråd med foretakets dokumenterte krav. For å motvirke avvik i IKT-systemene, som vil påvirke oppnåelsen av foretakets dokumenterte krav, skal foretaket gjennomføre regelmessige analyser og tiltak. Foretaket skal teste og dokumentere at driften fungerer i henhold til foretakets dokumenterte krav.

Beredskapstester
Finanstilsynet pekte i foreløpig rapport på at foretaket bør gjennomføre beredskapsøvelser der et cyberangrep er scenario og samtidig teste om kriseplanen er tilstrekkelig detaljert for dette scenarioet.

Finanstilsynet har merket seg opplysningene i styrets svar om at det ble gjennomført en beredskaps-test med et cyberangrep som scenario i januar 2023 og at foretaket også har planlagt en beredskaps-test med et slik test-scenario for 2024.

Finanstilsynet kommenterte at det ikke framgår om Vipps har en strategi for å sikre at Disaster Recovery (DR)-testene er dekkende, slik at alle funksjonsområdene med risiko sikres en regelmessig testing.

Fra styrets svar framgår det at foretaket vurderer hvor sannsynlig et risikoscenario er, samt mulige konsekvenser, og velger test-scenarioene basert på de mest relevante risikoene. Styret tar innspillene fra Finanstilsynet til etterretning og vil igangsette en utvidelse av relevante styrende dokumenter og rutiner, inkludert DR-strategien.

Finanstilsynet tar styrets svar til etterretning.

Sikkerhet
Ifølge IKT-forskriften § 5 skal foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. I tillegg skal det foreligge retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

Rutine for penetrasjonstesting
Finanstilsynet pekte i foreløpig rapport på at det ikke framgikk om foretaket har en rutine for gjennomføring av penetrasjonstesting som beskriver hvordan testingen skal gjennomføres inkludert krav til bruk av ulike leverandører for å sikre at sikkerheten i applikasjoner og infrastruktur testes og angripes på ulike måter.

Fra styrets svar har Finanstilsynet merket seg at gjennomføring av penetrasjonstesting er en del av foretakets sikkerhetsstesting som er kravstilt gjennom foretakets standarder for sikker utvikling og for sårbarhetshåndtering. Styret bekrefter videre at arbeidet med å kontinuerlig forbedre kravstilling og dokumentasjon av sikkerhetstestingen fortsetter.

Finanstilsynet tar styrets svar til etterretning.

Sensitiv betalingsinformasjon
I henhold til finansforetaksforskriften § 3-2 skal foretaket ha rutiner for lagring og overvåkning av sensitiv betalingsinformasjon, samt begrensninger i og oversikt over adgang til denne informasjonen.

Finanstilsynet pekte i foreløpig rapport på at Vipps viser til at sensitiv betalingsinformasjon i betalingskortdata lagres hos leverandøren. Finanstilsynet presiserte at det er Vipps som har ansvar for sikkerheten til den sensitive betalingsinformasjonen selv om lagringen er utkontraktert.

Finanstilsynet har fra styrets svar merket seg at Vipps bekrefter at foretaket selv er ansvarlig for sikkerheten av sensitiv betalingsinformasjon, også når lagringen av betalingskortdata er utkontraktert. Fra styrets svar framgår det at foretaket minimum årlig reviderer leverandørens etterlevelse av sikkerhetsstandarder for behandling av kortopplysninger i henhold til Payment Card Industry Data Security Standard PCI DSS, der leverandøren er sertifisert på høyeste sikkerhetsnivå.

Finanstilsynet tar dette og øvrige deler av styrets svar til etterretning.

Sikkerhet i applikasjonen på mobil
I henhold til finansforetaksforskriften § 3-2 skal foretaket ha retningslinjer knyttet til sikkerhet, inkludert en detaljert risikovurdering av betalingstjenestevirksomheten og en beskrivelse av kontrollen med sikkerheten. Videre plikter foretaket å ha tiltak for å beskytte brukerne av betalingstjenestene mot risikoene som er identifisert, inkludert svindel og ulovlig bruk av sensitive opplysninger og personopplysninger.

Finanstilsynet stilte i foreløpig rapport spørsmål til hvordan Vipps avdekker at sikkerheten på brukerens mobil er for dårlig til at Vipps kan brukes på den, inkludert om versjonen av operativsystemet er for gammel. Finanstilsynet ba Vipps sikre at det foreligger rutiner for å beslutte

at en versjon av operativsystemet(ene) er for gammel og for å sikre at Vipps ikke kan brukes på mobiler med for gammelt operativsystem.

Finanstilsynet har merket seg styrets svar hvor det framgår at Vipps har etablert operasjonelle prosesser for å fange opp kjente sikkerhetshull/-mangler knyttet til operativsystem og i den sammenheng vurderer om slike mangler gjør det nødvendig å gjøre Vipps utilgjengelig av sikkerhetshensyn. Foretaket mangler imidlertid systematisk dokumentasjon av vurderingene, og Vipps vil etablere rutiner for dette slik Finanstilsynet ber om.

Finanstilsynet tar styrets svar til etterretning.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Åshild Johnsen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.